



ORGANIZACIÓN DE AVIACION CIVIL INTERNACIONAL

PROYECTO RLA/06/901

**GUIA DE ORIENTACION PARA LA IMPLEMENTACION DE REDES NACIONALES
DIGITALES EN PROTOCOLO IP PARA APOYAR ACTUALES Y FUTURAS
APLICACIONES AERONAUTICAS**

La designación empleada y la presentación de este material en esta publicación no implican expresión de opinión alguna por parte de la OACI, referente al estado jurídico de cualquier país, territorio, ciudad o área, ni de sus autoridades, o a la delimitación de sus fronteras o límites.

INDICE

i. Índice	3
ii. Antecedentes.....	4
Consideraciones generales contribuyentes a la toma de decisiones.....	5
Business.....	5
Soporte industrial.....	5
Políticas de seguridad.....	5
Implantación.....	6
Capacitación.....	6
Consideraciones específicas de diseño y despliegue.....	6
Elecciones básicas.....	6
Gestión remota.....	9
Plan de direccionamiento.....	11
Transferencia de servicios.....	11
iii. Apéndice 1 – Conceptos de networking.....	1-1
iv. Apéndice 2 – Descripción de un router.....	2-1
v. Apéndice 3 – Protocolos de enrutamiento.....	3-1
vi. Apéndice 4 – Gestión de dispositivos.....	4-1

1. Antecedentes

1.1 Cuando el panel SICAS fue originalmente encargado del desarrollo de los SARP para la Red de Telecomunicaciones Aeronáuticas (ATN), el panel fue requerido para basar la ATN en los protocolos abiertos que fueren el “estándar industrial”, lo que dio lugar a la elección de los protocolos de la ISO, Open Systems Interconnection (OSI).

1.2 En aquel momento, el uso de este protocolo fue asignado por mandato por muchos Estados contratantes de ICAO. Antes de 1997, el panel y su sucesor, el ATNP, habían trabajado con éxito y se validaron los SARP para la ATN. Desde entonces, los usos de los servicios de tráfico aéreo (ATS) basados en estos SARP, se han movido hacia el despliegue y ahora se están utilizando operacionalmente en algunas áreas.

1.3 Sin embargo, aunque los protocolos de la ISO fueron apoyados fuertemente por los Estados contratantes, fuera de los servicios de comunicaciones aeronáuticos, los de la industria fueron convertidos usando un más viejo sistema de estándares que se conocen colectivamente como “TCP/IP” (más correctamente la Suite de Protocolos de Internet (IPS)). Éstos ahora son los estándares de hecho para las comunicaciones abiertas, y los productos basados en protocolos del IPS están extensamente disponibles y a un bajo costo.

1.4 En el ambiente de tierra, un ahorro en costes extremadamente significativo puede ser hecho introduciendo los productos basados en los protocolos IPS para la ayuda de ICAO, tales como el servicio de la manipulación de mensajes del ATS (ATSMHS), y otros en apoyo de comunicaciones aeroterrestres. Los Estados contratantes de ICAO han comenzado el despliegue del IPS en tales áreas.

1.5 En el ambiente aeroterrestre, hay interés en el uso del IPS. Sin embargo, esto es un ambiente muy diverso a la tierra. Hay trabajos específicos a hacer con respecto a la movilidad y la seguridad, que tienen que ser consideradas cuidadosamente. Mientras que hay un deseo de hacer uso de los estándares industriales en el ambiente aeroterrestre, esto se reconoce como más complejo, y su implementación durará por consiguiente más tiempo en comparación con el ambiente de tierra.

1.6 En consideración de las consideraciones antedichas, el Consejo de Navegación Aérea dirigió al grupo de trabajo I del ACP (Panel de Comunicaciones Aeronáuticas) a estudiar el uso del TCP/IP en el establecimiento de una red aeronáutica y la fabricación de las recomendaciones para el trabajo futuro en esta área.

1.7 El grupo de trabajo I del ACP progresó la tarea con la siguiente metodología:

1.7.1 Un examen por parte de los Estados miembros fue emprendido para determinar el grado que el IPS estaba siendo utilizado para las comunicaciones aeronáuticas en cada estado, y en qué contexto.

1.7.2 La consideración fue dada a los requisitos de comunicaciones aeronáuticas en áreas tales como funcionamiento, seguridad, movilidad, etc.

1.7.3 La consideración separada fue dada a la tierra-tierra y los ambientes aeroterrestres, y la capacidad de los productos “disponibles” existentes del IPS para cumplir estos requisitos.

1.7.4 Una conclusión entonces fue desarrollada, en la conveniencia del IPS para cumplir requisitos aeronáuticos de comunicaciones, y un programa de trabajo futuro propuesto fue formulado para facilitar el uso del IPS en el área seleccionada de comunicaciones aeronáuticas.

1.8 *La conclusión del informe del ACP es que el uso del IPS para apoyar la comunicación aeronáutica en el ambiente de tierra se justifica completamente.*

1.9

2. **Consideraciones generales contribuyentes a la toma de decisiones**

2.1 Business

2.1.1 La decisión para ejecutar el IPS debe ser una decisión económica así como una decisión técnica. Debe ser observado que mientras que los protocolos establecidos existentes del IPS están libres de restricciones de la patente y disponibles sin carga, esto puede no ser verdad para los protocolos futuros.

2.1.2 Hay una población grande de vendedores y de proveedores de servicios para los servicios del equipo y del establecimiento de una red del IPS. Esto ha creado un ambiente competitivo que debe permitir a Estados contratantes de OACI obtener la tasación favorable cuando está comparado al equipo y a los servicios en red.

2.2 Soporte industrial

2.2.1 Hay una gran cantidad de compañías que proporcionan el equipamiento en red y servicios basados en IPS, mientras que el establecimiento de una red de la OSI gradualmente disminuye su capacidad de soporte. Además, los estándares del IPS son mantenidos por el Internet Engineering Task Force (IETF) con la ayuda activa de la industria.

2.2.2 El número de nodos desplegados para el IPS está en los diez millones, mientras que las redes WAN basadas en OSI no se despliegan en esta escala, y los se han desplegado se están substituyendo por el IPS.

2.3 Políticas de seguridad a considerar

2.3.1 El establecimiento de una red IPS aumenta la necesidad de la seguridad eficaz; esto es debido a la misma franqueza del IPS. La oscuridad de los protocolos de ISO/OSI debido al hecho de que no estén desplegados extensamente en redes, proporciona una cantidad determinada de protección.

2.3.2 Los ataques contra redes del IPS se publican bien, y los piratas informáticos gastan mucha energía hacia la concepción de nuevas formas de ataque. El coste de un sistema capaz de infligir daño importante en una red puede estar tan solo en una computadora barata que apoye el IPS.

2.3.3 Esto significa que los sistemas del ATS usando el IPS, sin mecanismos de seguridad eficaces, serían vulnerables a las varias formas de violación de seguridad. Por lo tanto se recomienda que los servicios de seguridad existentes subyacentes del análisis ATN de la vulnerabilidad estén puestos al día para reflejar el uso del IPS.

2.3.4 Hay numerosos mecanismos de seguridad que se pueden utilizar en una red IPS. Los sistemas actuales pueden utilizar el protocolo de la seguridad del IP (IPSec) para asegurar seguridad de la capa de red y/o el protocolo de SSL/TLS para asegurar seguridad de la capa de transporte del IPS. IPSec puede proporcionar servicios de encriptación y/o de autenticación.

2.3.5 Por otra parte, la Administración Aeronáutica de cada Estado deberá observar su incumbencia interna en las Políticas de Seguridad de la Información dictadas por sus propios gobiernos.

2.3.6 Es recomendable la lectura de la Norma “Information Technologies – Security techniques – Codes of practice for information security management “ISO-IEC 17799, del año 2005, publicado por la ISO (International Standardization Organization) y la IEC (International Electrotechnical Commission). La última versión, BS ISO IEC 17799: 2005 reemplaza a las versiones más viejas de los estándares BS 7799 e ISO 17799. Está basada en el British Standard 7799. Aunque la norma ISO 17799 no es de cumplimiento obligatorio, *proporciona una base sólida para un programa de seguridad de la información.*

2.3.7 Asimismo, deberá contemplarse lo estipulado en el *Manual de Disposiciones Técnicas de la Red de Telecomunicaciones Aeronáuticas (ATN)* de la OACI (Doc 9705) y las listas de verificación de auditoría de seguridad (Information Security Management BS 7799.2:2005 Audit Check List for SANS).

2.4. Implantación

2.4.1 Puesto que el IPS es el estándar mundial de facto del establecimiento de una red, con muchos años de despliegue detrás de él, hay una población grande de ingenieros experimentados en establecimiento de redes, disponibles para apoyar la puesta en práctica. Esta base de conocimiento puede apoyar el despliegue de una ATN basada en IPS.

2.5 Capacitación

2.5.1 No obstante lo antedicho, es imprescindible iniciar rápidamente un esquema de capacitación y/o certificación en redes IPS, que permita al Estado contar con el mínimo número de personas que puedan contribuir a instalar, habilitar, gestionar y mantener la red IPS en forma satisfactoria.

3. **Consideraciones específicas de diseño y despliegue**

3.1 Decisiones básicas para el diseño preliminar de la red nacional

3.1.1 La recomendación básica que debiera atender cada Estado es que la red IPS *debe ser exclusivamente privada.*

3.1.2 Cada estado podrá seleccionar el *proveedor* de los *elementos IPS* que estime conveniente; sin embargo, deberá considerar que esa elección debe ser prácticamente definitiva, ya que no es recomendable de ninguna manera disponer de equipamiento con idéntico fin, pero de diferentes marcas, ya que este hecho obligara a *multiplicar* innecesariamente:

3.1.2.1 La capacitación.

3.1.2.2 Los repuestos.

3.1.2.3 Los recursos humanos.

3.1.2.4 La gestión remota.

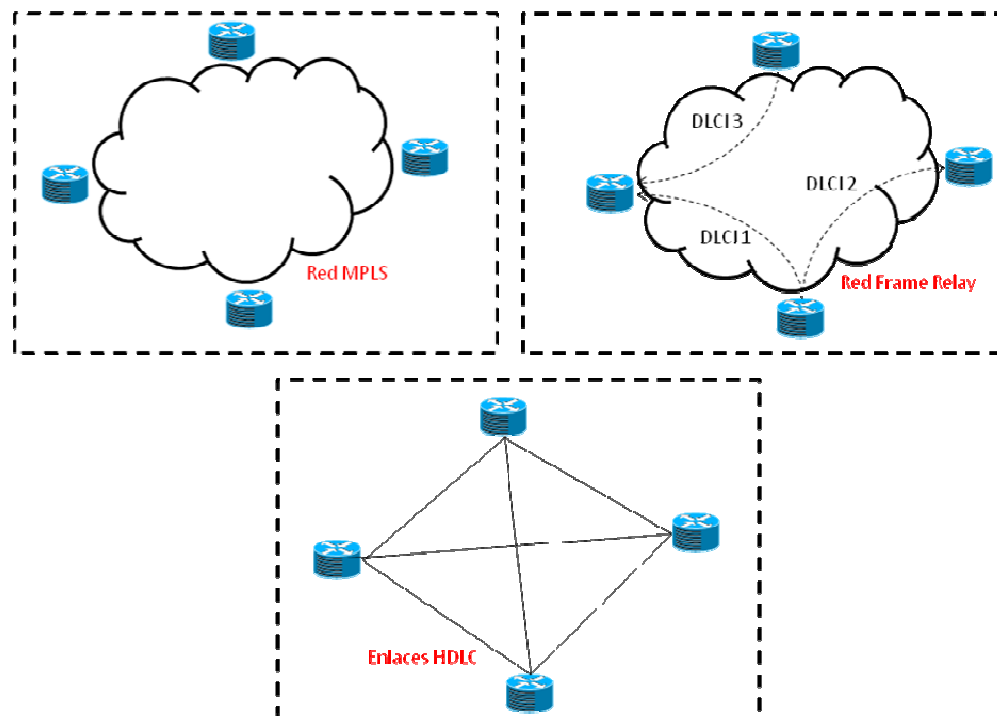
3.1.3 Asimismo, es una decisión de cada Estado (basada en sus políticas técnicas y económicas) elegir si la red IPS deberá ser:

3.1.3.1 Soportada por *redes terrestres o satelitales* (o bien un mix de ambas).

3.1.3.2 Basada en una red de enlaces *propios o arrendados* a las PTTs (*).

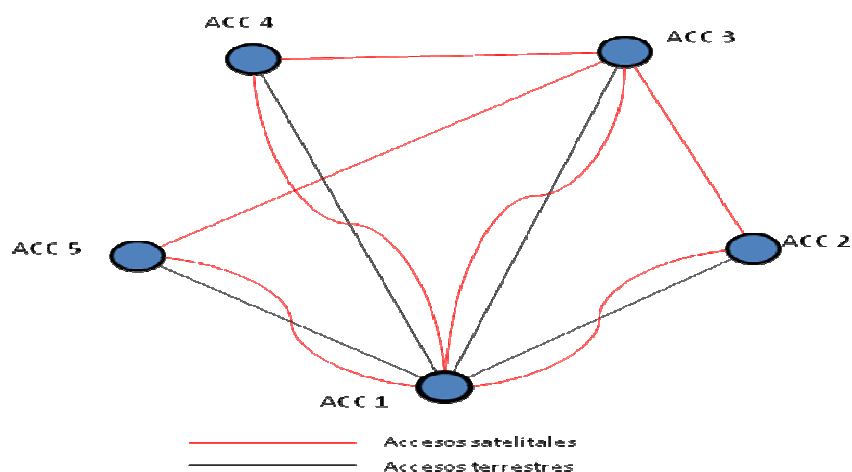
3.1.3.3 Transportada sobre líneas dedicadas o conexiones conmutadas. Las conexiones conmutadas, a su vez, pueden ser de circuitos conmutados o de paquetes/celdas conmutadas (*).

FIGURA 1: MPLS, Frame Relay y HDLC



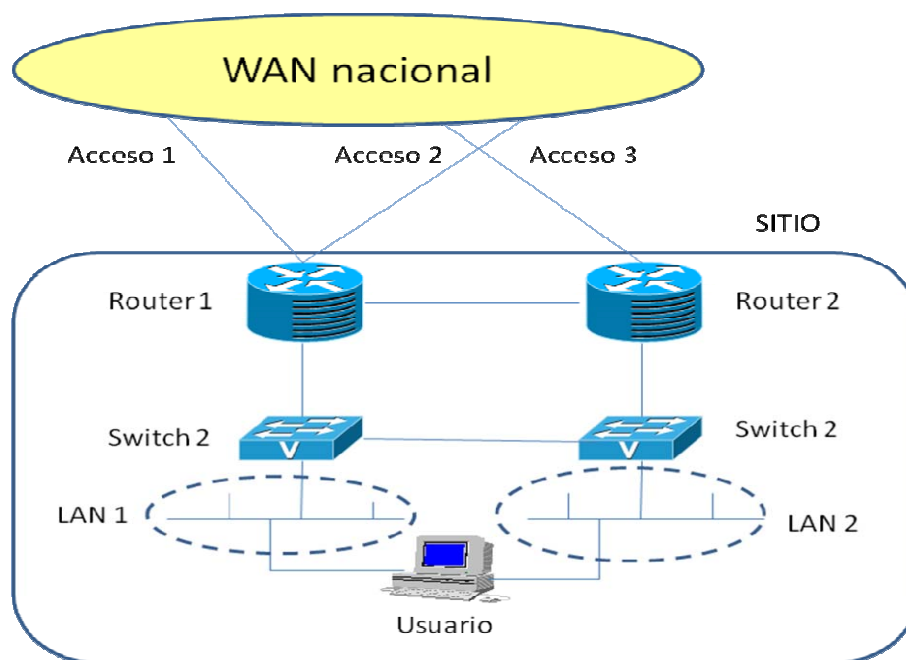
3.1.3.4 Si se utiliza punto a punto, *accesos* a la WAN (red de área ampliada) *simples* o *duplicados* en cada uno de los sitios donde llega, Ver Figura 2 (*).

FIGURA 2: EJEMPLO DE RED IP, HDLC, ACCESOS REDUNDANTES



3.1.3.5 Con *elementos de networking simples o duplicados* (Ver Figura 3).

Figura 3: Elementos de networking redundados



(*): Estos asuntos se tratan extensamente en el Apéndice 1.

En el *Apéndice 1 “Conceptos de networking”* se pormenorizan los distintos aspectos contribuyentes al diseño y configuración de una red, así como todo lo relativo a los elementos de segmentación de datos que la constituyen (*routers* y *switches*).

En el *Apéndice 2 “Descripción de un router”*, se detallan todos los aspectos constructivos, funcionales y técnicos de un router.

En el *Apéndice 3 “Protocolos de enrutamiento”* se detallan aspectos relativos al enrutamiento.

NOTA: en todos los Apéndices se hace referencia extensiva a elementos Cisco, sin que con ello se pretenda influir en la elección de cada Estado en los elementos a ser instalados.

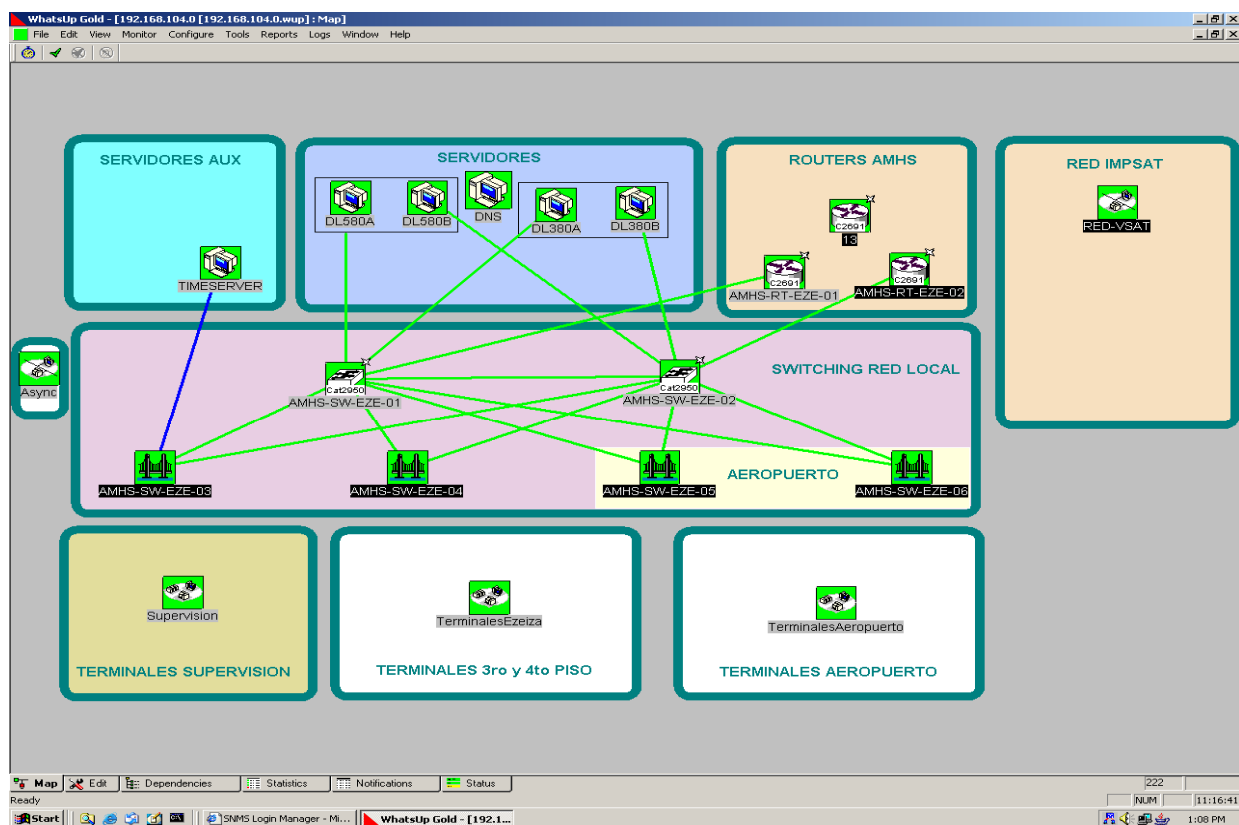
3.2 Gestión remota de la red

3.2.1 La red deberá ser instalada de forma de tal de permitir la visualización y gestión remota de *todos y cada uno de sus componentes*.

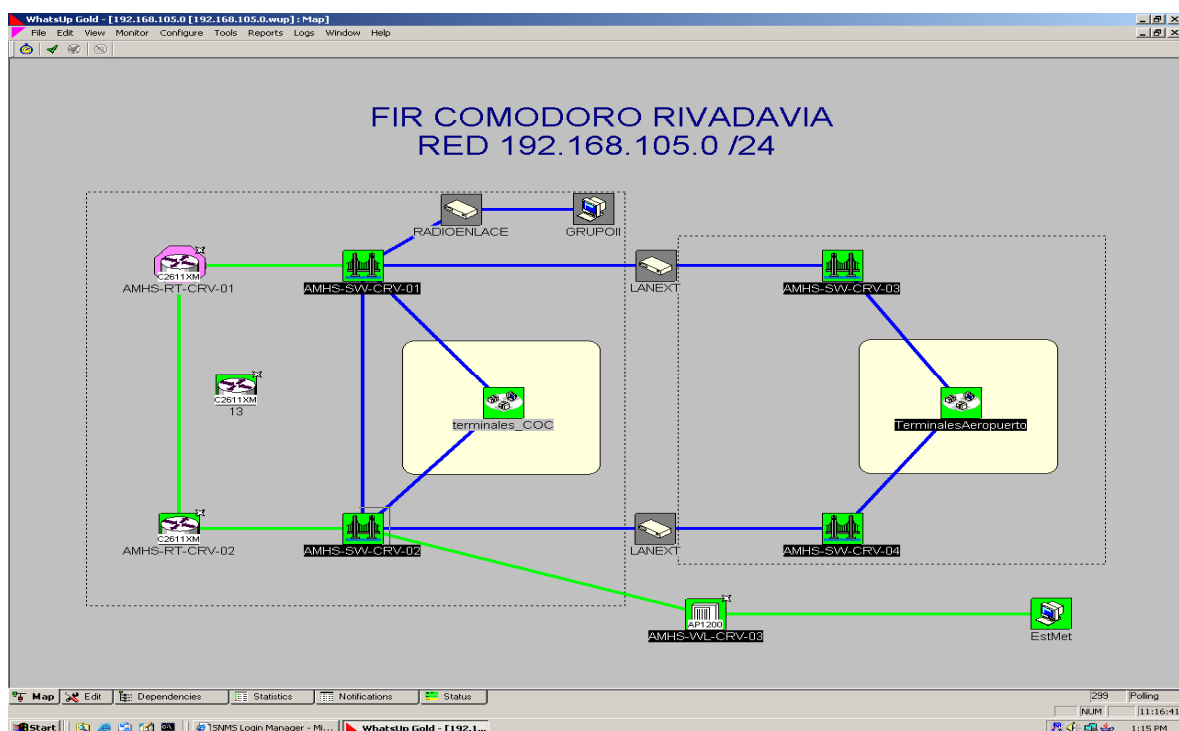
En el *Apéndice 4 “Paquete de gestión de dispositivos”* se exponen los elementos de gestión disponibles y su inserción en el funcionamiento de la red IPS.

3.2.2 En las figuras siguientes se exponen ejemplos de visualización de los elementos de red correspondientes a:

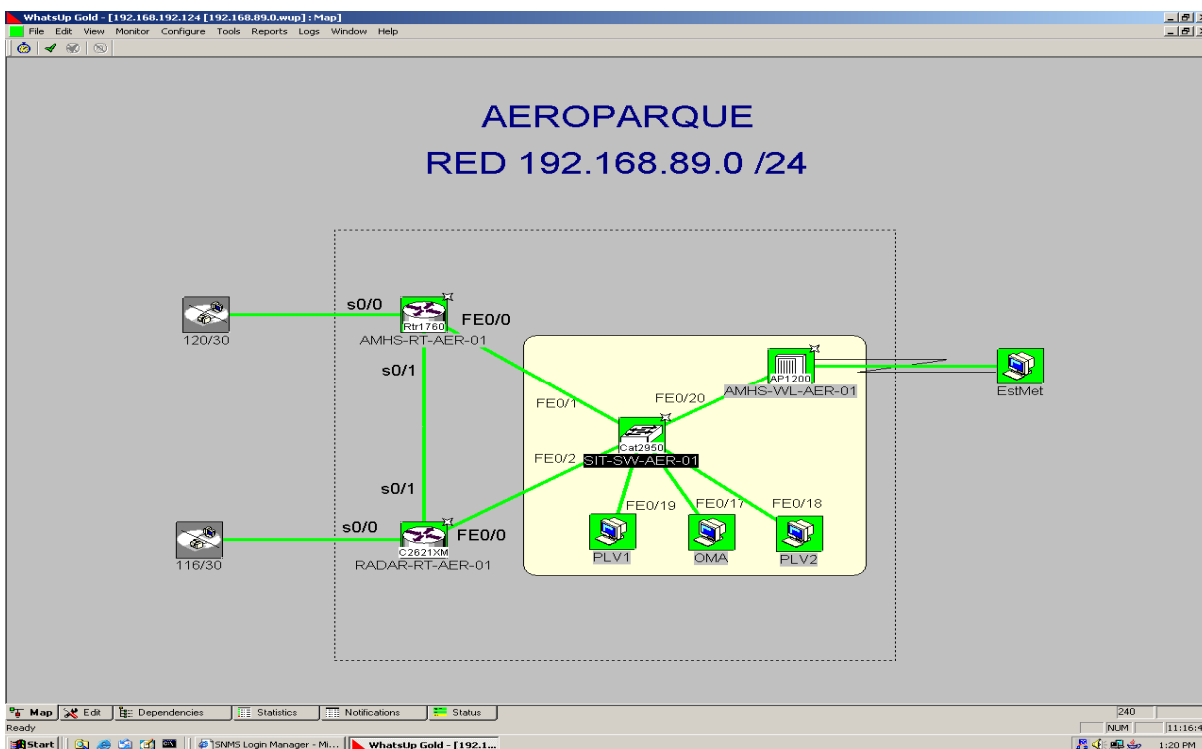
3.2.2.1 La sede central de un servicio AMHS



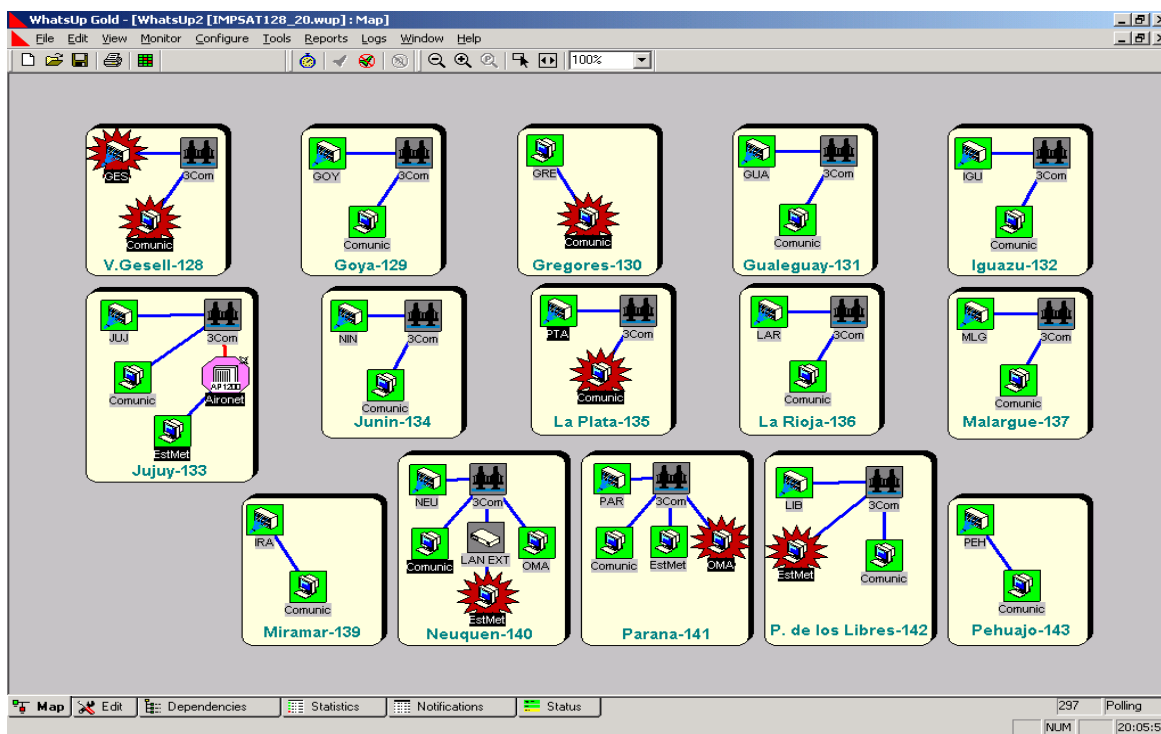
3.2.2.2 Un ACC, bajo la concepción de “inexistencia de punto común de falla”.



3.2.2.3 Un aeropuerto de gran movimiento



3.2.2.4 Un grupo de pequeños aeropuertos



3.3. Plan de direccionamiento

3.3.1 Cada Estado podrá utilizar las direcciones y el esquema de direccionamiento que prefiera, pero es recomendable:

3.3.1.1 Que las direcciones de red sean asignadas en bloques continuos.

3.3.1.2 Que la distribución de bloques de direcciones se realice en forma jerárquica, de forma tal de permitir la escalabilidad de ruteo.

3.3.1.3 Que sea posible poder configurar subredes, para poder aprovechar así al máximo cada red asignada.

3.3.2 Las únicas direcciones asignadas y conocidas por el resto de los Estados serán las de las interfaces de los equipos de comunicaciones utilizados en las fronteras de interconexión entre las redes internas y externas a cada Estado.

3.3.3. De esta forma cada estado deberá garantizar el ruteo a través de su red hacia la/s dirección/es internas de los servidores de aplicación que utilice contra otros Estados.

3.3.4 La Oficina Regional de la OACI se encargará de determinar cual de las opciones de *ruteo regional* será la seleccionada finalmente, como asimismo coordinara y asignara las direcciones y modalidad que se establezca, en virtud de los arreglos institucionales correspondientes (Grupo de Tareas ATN, Comité CNS, Grepecas, ACP, etc.)

3.4 Transferencia de servicios

3.4.1 A fin de no perturbar el normal desarrollo de las operaciones aéreas, es recomendable que los servicios se muden a la red IPS de a uno por vez, y paulatinamente. Tal como fue largamente establecido, el *AMHS* **debe** ser primer servicio a ser montado sobre la ATN basada en IPS.

3.4.2 Una vez completado el despliegue de este servicio en particular, cada Estado podrá elegir entre:

3.4.2.1 Continuar con otros servicios de datos (señales radar, aplicaciones AIS y/o MET, AIDC, OLDI, etc.).

3.4.2.2. Iniciar la transferencia de servicios operacionales de voz (comunicaciones ATS directas o conmutadas).

3.4.2.3 Un mix entre las dos opciones mencionadas.

3.4.3 *Señales radar*: si estas son generadas en forma IP nativa, se montaran directamente, según el direccionamiento correspondiente. Si son generadas en forma serial sincrónica, ya sea esta V.35 o V.24, deberá ingresárselas a la red en forma “multicast”, a fin de ser recibidas en los destinos necesarios.

3.4.4 *AIDC*: esta aplicación deberá ser “montada” encima de la aplicación AMHS, por lo que su transporte por la red IP es inmediato.

3.4.5 *OLDI*: para los Estados que dispongan del servicio OLDI X.25 en lugar del AIDC, es recomendable efectuar los arreglos de software necesarios para que el mismo sea transportable vía IP en lugar de X.25.

3.5.6 *Comunicaciones orales ATS (ACC – TWR o entre ACCs del mismo estado)*: es recomendable iniciar las pruebas pre operacionales duplicando circuitos convencionales con aeropuertos de gran densidad de tráfico, a fin de detectar / corregir los inconvenientes que pudieren surgir. Una vez finalizada esta etapa, se deberán desafectar los convencionales y ampliar el uso hacia el resto de la red.

3.4.7 *Comunicaciones orales ATS (entre ACCs de distintos estados)*: vía REDDIG, una vez efectuados los arreglos bi o multilaterales necesarios.

3.4.8 *ADS –B*: cuando se disponga de este servicio.

INDICE

NETWORKING

REDES LAN - ETHERNET

PROTOCOLOS DE LAN

TECNOLOGÍAS ETHERNET

DISPOSITIVOS DE LAN

VLANS

REDES WAN

REDES Y DISPOSITIVOS WAN

SERVICIOS WAN

PROTOCOLOS DE ENCAPSULACIÓN WAN

PROTOCOLOS TCP/IP

FUNDAMENTOS DE REDES

PROTOCOLO IP (RFC791-RFC760)

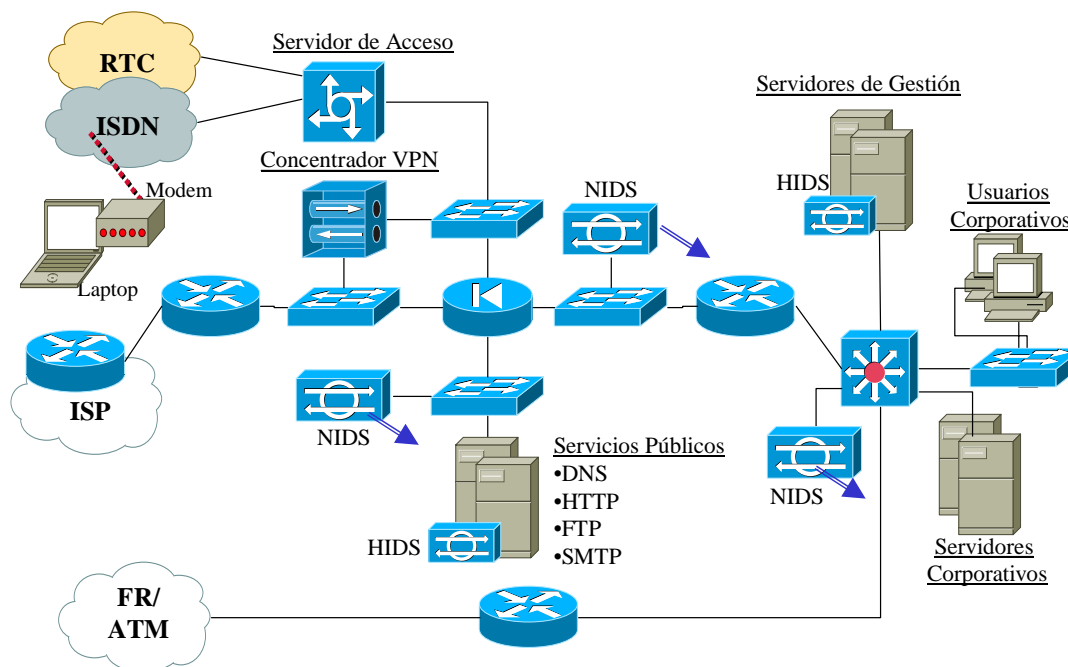
TCP

ICMP

SWITCHING Y ROUTING

1. NETWORKING

1.1 El término networking (ó también internetworking) se aplica a la industria, productos y a las actividades relacionadas con la interconexión, diseño y administración de las redes individuales, de manera que pasan a funcionar y comportarse como una única gran red.



1.2 En la figura se muestra el diagrama de una red corporativa de mediano porte. En ella se muestran los dispositivos de uso frecuente en las redes. De manera general, los objetivos de diseño de una red son:

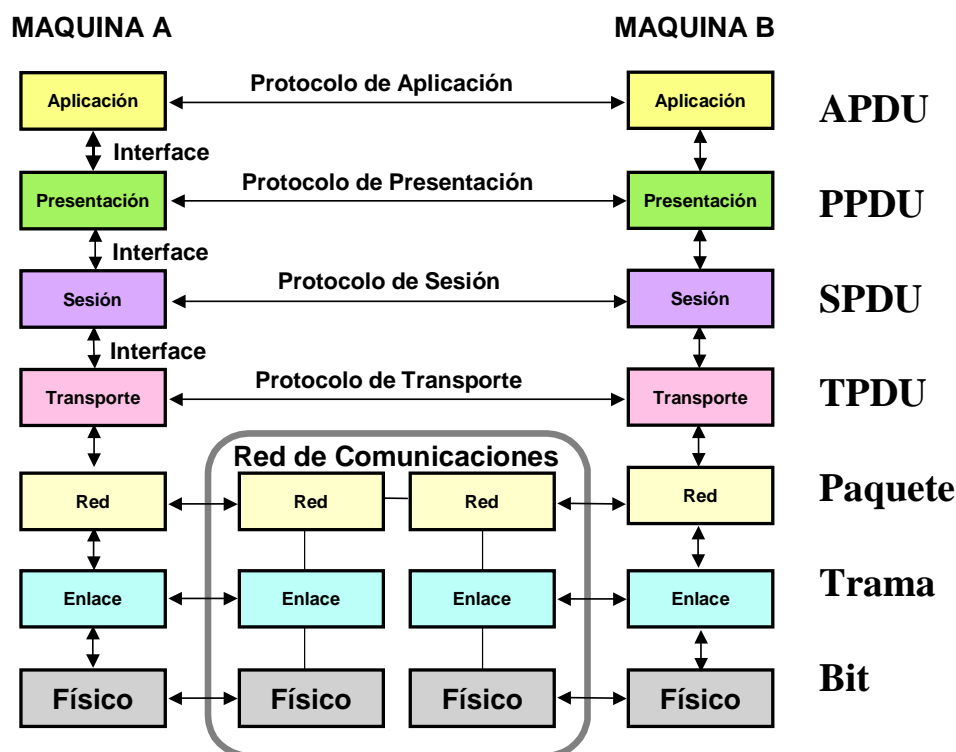
- 1.2.1 Funcionalidad
- 1.2.2 Performance
- 1.2.3 Seguridad
- 1.2.4 Gestión
- 1.2.5 Escalabilidad
- 1.2.6 Compatibilidad

Modelos de referencia

1.3 Los modelos de referencia proveen la ventaja de dividir la complejidad de las operaciones de la red en un conjunto manejable de niveles o capas. El diseño de protocolos en base a los modelos de referencia posibilita la introducción de cambios en una capa, sin que las otras se vean afectadas. Es un instrumento eficaz para analizar todo tipo de redes.

Modelo de referencia OSI

1.4 El modelo de referencia OSI es un marco de trabajo desarrollado por la ISO para promover la estandarización de los protocolos utilizados en la interconexión de sistemas heterogéneos (abiertos).



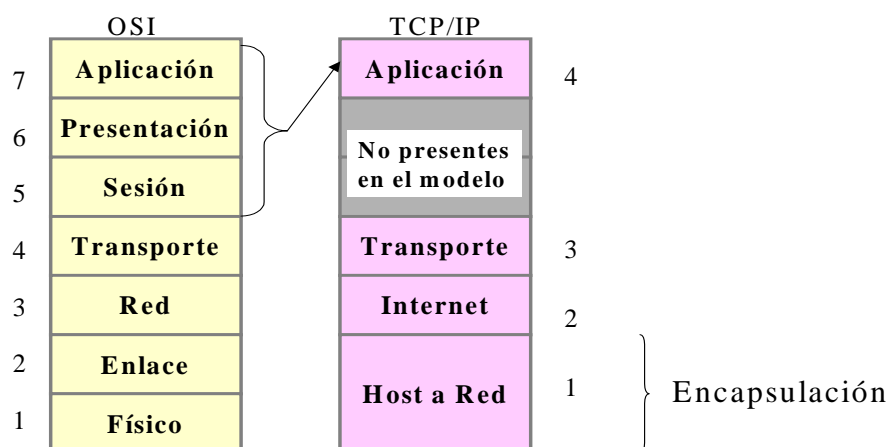
CAPA OSI	DESCRIPCIÓN FUNCIONAL	EJEMPLOS
7.- APLICACIÓN	Semántica. Interface con las aplicaciones/usuarios.	Telnet, HTTP, FTP, www, NFS, SMTP, SNMP, X.400
6.- PRESENTACIÓN	Formato de los datos. Sintaxis. Procesamientos especiales (encriptación).	JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, MIDI
5.- SESIÓN	Flujo ordenado de los datos entre las partes intervinientes (transacciones).	RPC, SQL, NFS, nombres NetBios, AppleTalk ASP, DECnet SCP
4.- TRANSPORTE	Calidad de servicio. División entre red y capas sup. Mux.	TCP, UDP, SPX
3.- RED	Direccionamiento lógico. Enrutamiento.	IP, IPX, APPLETALK, ICMP
2.- ENLACE DE DATOS	Acceso al medio. Enlace entre estaciones vecinas. Manejo de Errores.	IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, IEEE 802.5/802.2
1.- FÍSICA	Señales físicas. Conectores. Temporización.	EIA/TIA-232, V.35, EIA/TIA-449, V.24, RJ-45, Ethernet, 802.3, 802.5, FDDI, NRZI, NRZ, B8ZS ¹

¹ Atención: frecuentemente estas especificaciones se complementan (ej: RJ-45 es solamente el conector).

Modelo de referencia TCP/IP

1.5 En el modelo TCP/IP no existen las capas de presentación y sesión. Directamente sobre la capa de transporte se encuentra la capa de aplicación, la cual contiene todos los protocolos de alto nivel.

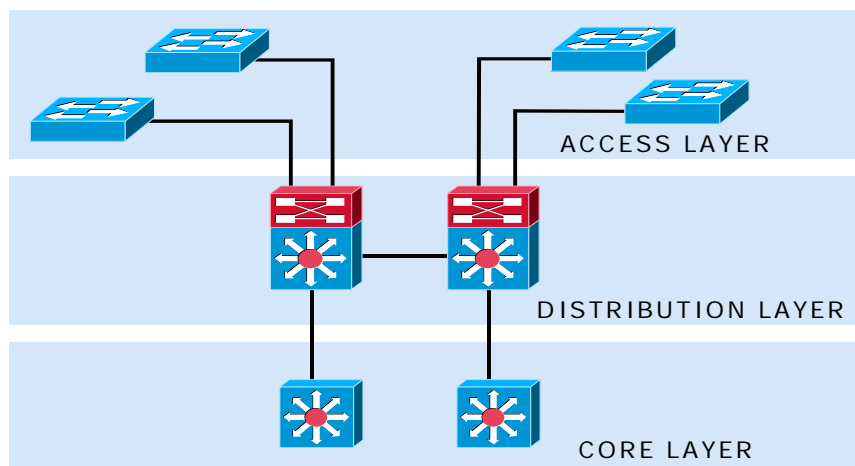
1.6 Un gran vacío (y por ende gran flexibilidad) existe por debajo de la capa internet en el modelo TCP/IP, dado que no define ningún protocolo (solamente menciona que el host debe conectarse a la red utilizando algún protocolo para enviar los paquetes).



1.7 Siempre que se hable del modelo de capas (a menos que se indique lo contrario), se utilizará el modelo de referencia OSI. Así, todo el mundo sabe que IP es un protocolo de capa 3 (nótese que en el modelo TCP/IP corresponde a la capa 2).

Modelo jerárquico CISCO

1.8 Con las mismas ventajas de la modelización en capas de OSI, y otras orientadas a las implementaciones prácticas de redes Campus, CISCO posee su propio diseño jerárquico - facilidad de operación y administración, mejor comprensión, escalabilidad, implementación de políticas, eficacia del direccionamiento y resolución de problemas-.



1.9 En el siguiente cuadro se resumen las características de cada una de las capas del modelo jerárquico:

CAPA CISCO	DESCRIPCIÓN
CORE	Transporte de alta velocidad, elevada confiabilidad, redundancia y baja latencia. Conexiones entre sitios. Switches de alta velocidad. No comprimir, filtrar, encriptar u otras cargas de procesamiento.
DISTRIBUTION	Listas de acceso, listas de distribución, sumarización de rutas, enrutamiento de VLANs, políticas de seguridad, filtros, agregación, encriptación, compresión y calidad de servicio. Routers de alta velocidad y switches de capa 3.
ACCESS	Servicios de acceso remoto, acceso local shared y switched, filtrado de direcciones MAC y segmentación. Agregación de VPN's. Switches de acceso.

Bases numéricas

1.10 El estudio de las direcciones físicas y lógicas exige el repaso de las bases y conversiones numéricas. En el siguiente diagrama se muestra el principio de formación de los números en diferentes bases.

b^n	b^7	b^6	b^5	b^4	b^3	b^2	b^1	b^0	base
...	10^7	10^6	10^5	10000	1000	100	10	1	$b=10$
...	128	64	32	16	8	4	2	1	$b=2$
...	8^7	8^6	32768	4096	512	64	8	1	$b=8$
...	16^7	16^6	16^5	65536	4096	256	16	1	$b=16$

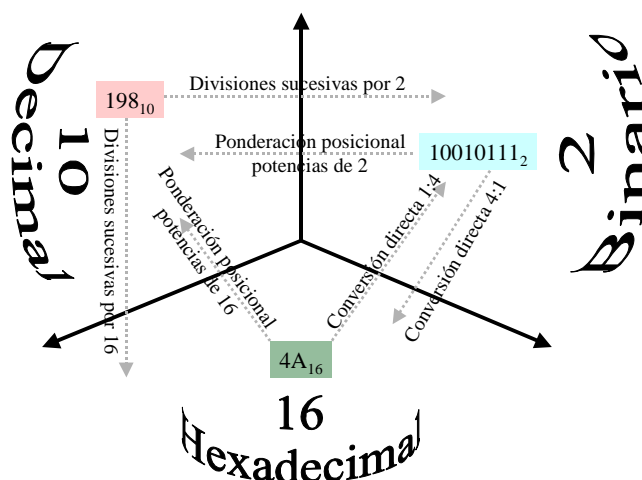
Base decimal: 0 1 2 3 4 5 6 7 8 9

Base binaria: 0 1

Base octal: 0 1 2 3 4 5 6 7

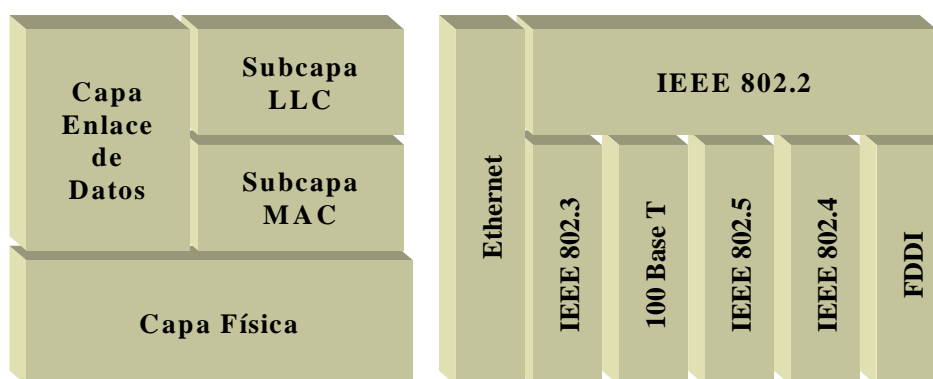
Base hexadecimal: 0 1 2 3 4 5 6 7 8 9 A B C D E F

1.11 Las claves para las conversiones entre diferentes bases está representada por:



2. PROTOCOLOS DE LAN

2.1 Los protocolos de LAN funcionan en las dos capas más bajas del modelo de referencia OSI.



2.2 El IEEE (Institute of Electrical and Electronic Engineers) diferencia la capa de enlace en dos subcapas: MAC (Media Access Control) y LLC (Logical Link Control). La subcapa MAC permite e instrumenta el acceso al medio, tal como el método de contención o token passing, mientras que la subcapa LLC se encarga del framing, control de flujo, control de errores y direccionamiento de subcapa MAC.

Métodos de acceso al medio

2.3 Los protocolos de LAN, típicamente usan uno de dos métodos para acceder al medio físico de la red: CSMA/CD (Carrier Sense Multiple Access/Collision Detect) y Token-passing. En el esquema CSMA/CD los dispositivos de la red contienen por el uso del medio físico. Por ello se denomina acceso por contención. Los ejemplos más característicos de redes LAN que utilizan CSMA/CD son Ethernet/IEEE 802.3, incluyendo 100BaseT.

2.4 En el esquema de acceso al medio Token-Passing, los dispositivos de la red acceden al medio físico en base a la posesión de una ficha (token). Los ejemplos más característicos son Token Ring/IEEE 802.5 y FDDI (Fiber Distributed Data Interface).

Nombre	Subcapa MAC	Subcapa LLC	Comentarios
Ethernet_II (DIX)	Ethernet	No existe diferenciación	Especificación propietaria de Digital, Intel y Xerox.
IEEE Ethernet	IEEE 802.3	IEEE 802.2	Conocida como Ethernet 802.3
Token-Ring	IEEE 802.5	IEEE 802.2	Originario de IBM

FDDI	ANSI X3T9.5	IEEE 802.2	Sin comentarios
------	-------------	------------	-----------------

Métodos de transmisión

2.5 Las transmisiones en las LAN corresponden a tres clasificaciones: *unicast*, *multicast* y *broadcast*. En los cuales una trama se envía a uno o más nodos.

2.5.1 En la transmisión *unicast* un único paquete es enviado desde un origen a un destino.

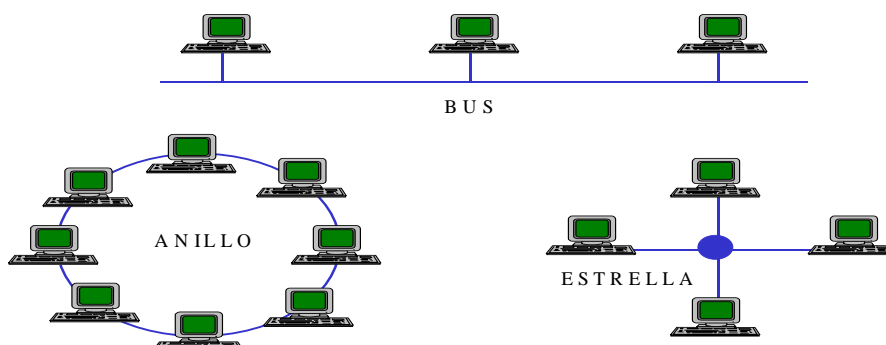
2.5.2 En *multicast*, un único paquete generado por un nodo origen, es copiado y enviado a un subconjunto especificado de nodos de la red.

2.5.3 La transmisión *broadcast* consiste en un único paquete copiado y enviado a todos los nodos de la red. El nodo origen genera un único paquete utilizando la dirección broadcast.

Topologías de LAN

2.6 Las topologías de LAN definen la forma en la que se organizan los dispositivos dentro de la red.

2.7 Existen tres topologías comunes: **bus**, **ring (anillo)** y **star (estrella)**.



2.8 Aunque estas topologías son arquitecturas lógicas, los dispositivos reales no necesitan estar físicamente organizados de acuerdo con estas configuraciones. Las topologías lógicas bus y ring, por ejemplo, suelen organizarse físicamente como una estrella (mediante un hub).

2.9 Las implementaciones más utilizadas de Ethernet (incluyendo Fast Ethernet, GigaEthernet y 10 GE) emplean una *topología de bus*, aún cuando aparentemente la topología física que se implementa a través de hubs y switches se presenta como estrella.

3. TECNOLOGÍAS ETHERNET

3.1 Ethernet ha sobrevivido, en su batalla inicial, como una tecnología de medio físico esencial a causa de su tremenda flexibilidad y relativa simplicidad de implementación y comprensión. Hoy, sin duda, es la tecnología de red LAN cómodamente dominante.

3.2 El término Ethernet se aplica a la familia de implementaciones LAN, las cuales incluyen:

Estándar	Subcapa MAC	Segmento Max (metros)	Tipo de Cable	#Pares
10Base5	802.3	500	50 ohm thick	-

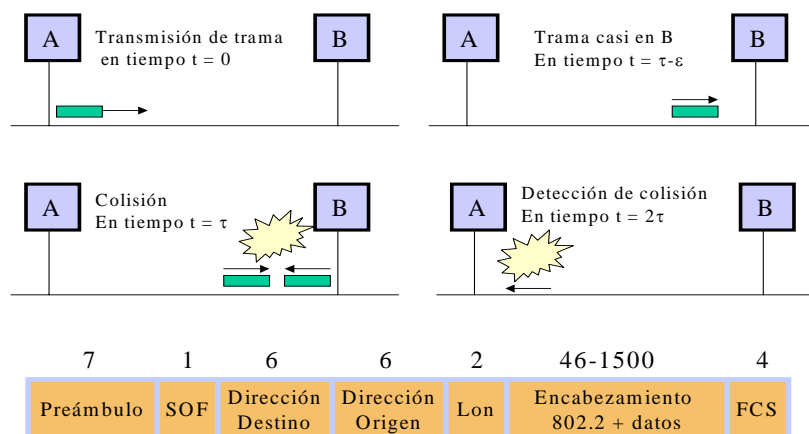
Estándar	Subcapa MAC	Segmento Max (metros)	Tipo de Cable	#Pares
10Base2	802.3	185	50 ohm thin	-
10BaseT	802.3	100	UTP 3-4-5	2
10BaseFL	802.3	2000	FO	1
100BaseFL	802.3u	100	UTP 5	2
100BaseFL	802.3u	100	UTP 3	4
100BaseFL	802.3u	100	UTP 3-4-5	2
100BaseFL	802.3u	400/2000	FO multimodo	1
100BaseFL	802.3u	10000	FO monomodo	1
1000BaseSx	802.3z	220-550	FO multimodo	1
1000BaseLx	802.3z	3000	FO	1
1000BaseCx	802.3z	25	STP	2
1000BaseT	802.3ab	100	UTP 5	2
10GBaseE ²	802.3ae	40000	FO monomodo	1

Ethernet e IEEE 802.3

3.3 Ethernet es una especificación de LAN en banda base inventada por Xerox Corp., para operar a 10 Mbps, utilizando CSMA/CD, sobre cable coaxil. El diseño fue creado para servir en redes con requerimientos esporádicos de altas cargas de tráfico. La especificación IEEE 802.3 fue desarrollada en base a Ethernet. IEEE 802.3 provee una gran variedad de opciones de cableados (por ejemplo 10Base5: en la cual 10 es la velocidad en Mbps., Base el método de señalización banda base, y 5 el tipo de medio físico coaxil).

3.4 En el ambiente broadcast de Ethernet, todas las estaciones “ven” todos las tramas que se transmiten sobre la red. Cada estación debe examinar las tramas para determinar si les han sido destinadas, en cuyo caso dichas tramas son pasadas hacia la capa superior.

² Existen otros estándares para FO mono y multimodo.



3.5 Cualquier estación sobre una LAN CSMA/CD puede acceder al medio físico en cualquier momento pero, antes de enviar datos, las estaciones verifican (“escuchan”) si no existen transmisiones en el medio. Si el medio está inactivo, puede iniciar la transmisión de sus datos.

3.6 Ocurre una colisión si dos o más estaciones comienzan la transmisión al mismo tiempo, en cuya situación ambas transmisiones resultarán dañadas y será menester retransmitir después de cumplido un cierto tiempo de back-off impuesto por un algoritmo que ejecutan las estaciones.

3.7 Los campos de la trama IEEE 802.3 son:

3.7.1 *Preámbulo*: Patrón alternante de unos y ceros para indicar a las estaciones la presencia de una trama.

3.7.2 *SOF* (Comienzo de trama): byte de delimitación para sincronizar la recepción de la trama.

3.7.3 *Direcciones de Destino y Origen*: Los tres primeros bytes de la dirección están especificados por el IEEE identificando al fabricante. Los últimos tres bytes los configura el fabricante. La dirección de origen es siempre unicast (un nodo), pero la dirección de destino puede ser unicast, multicast (grupo) o broadcast (todos los nodos).

3.7.4 *Longitud*: El número de bytes de datos que siguen a este campo.

3.7.5 *Datos*: Si los datos en el frame son insuficientes para llenar el campo a su mínimo valor de 64 bytes, se insertan bytes de padding para asegurar por lo menos una longitud de 64 bytes.

3.7.6 *FCS* (Frame Check Sequence): Es un valor CRC de 4 bytes para implementar el control de errores.

100-Mbps Ethernet (IEEE 802.3u)

3.8 Esta tecnología de LAN de alta velocidad ofrece una actualización importante en el ancho de banda disponible. 100BaseT es la especificación de la implementación 100 Mbps Ethernet sobre UTP y STP.

3.9 La subcapa MAC es compatible con IEEE 802.3, de manera que se mantiene el formato, tamaño y mecanismos de detección de errores, a la vez que soporta todas las aplicaciones y software de red de las redes 802.3.

3.10 100BaseT soporta ambas velocidades 10 y 100 Mbps, pero el diámetro máximo de la red queda reducido aproximadamente 10 veces respecto a 10BaseT (de 2000 a 205 metros), debido a la necesidad de detectar las colisiones dentro del tiempo necesario para transmitir un frame de longitud mínima de 64 bytes, aunque las estaciones se encuentren en los extremos de la red.

1 Gigabit Ethernet

3.11 1 GE es una extensión del estándar IEEE 802.3, la cual ofrece 1 Gbit/s de ancho de banda, manteniendo la compatibilidad con los dispositivos de red Ethernet y Fast Ethernet.

3.12 1GE provee un nuevo modo operativo full-dúplex para conexiones switch-to-switch y switch-to-station. Sin embargo, utiliza el mismo formato y tamaño de trama, y objetos de gestión de las redes IEEE 802.3.

3.13 Esta red ha sido diseñada para operar sobre fibra óptica, pero podrá ser implementada sobre UTP 5 y cable coaxil. El Grupo de Trabajo IEEE 802.3 formó a la Fuerza de Tareas 802.3z Gigabit Ethernet para desarrollar los estándares. El objetivo fue permitir operaciones full y half dúplex a 1 Gbps., de conformidad con el formato de frame tradicional y el método CSMA/CD de acceso al medio. También se prevé compatibilidad retroactiva con 10BaseT y 100BaseT.

3.14 Además el estándar especifica el soporte de enlaces de fibra multimodo con una longitud máxima de 500 metros, enlaces de fibra monomodo de hasta 2 Km, y enlaces de cobre de 25 metros como mínimo.

10 Gigabit Ethernet

3.15 La especificación de Ethernet a 10 Gigabit (10GE) es significativamente diferente en varios aspectos, a los primeros estándares Ethernet, principalmente en que solamente provee soporte para fibra óptica y opera en modo full-duplex. Lo cual significa que los protocolos de detección de colisiones no son necesarios.

3.16 Pero a pesar de escalar a 10 Gigabits por segundo, Ethernet conserva el formato de la trama y las capacidades actuales, de forma tal que no torna obsoletas a las inversiones en infraestructura de redes. 10GE es interoperable con otras tecnologías de networking, tales como SDH, haciéndose posible el tránsito de tramas Ethernet sobre trayectos SDH con muy alta eficiencia.

3.17 La expansión de Ethernet para su uso en redes de área metropolitana impulsa aún más el avance que la tecnología había experimentado con las redes a 1 Gbps., haciendo posible las conexiones Ethernet de extremo-a-extremo. Ethernet a 1 Gigabit ya ha sido desarrollada como tecnología de backbone para las redes metropolitanas con fibra oscura. Con las interfaces 10GE, transceptores ópticos y fibra monomodo, los proveedores de servicios podrán construir enlaces con un alcance mayor a los 40 Km.

4. DISPOSITIVOS DE LAN

4.1 Los dispositivos de red más utilizados son:

Repeaters

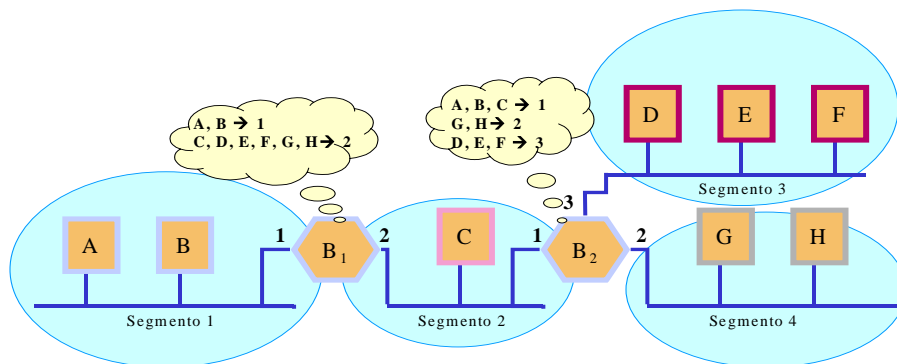
4.2 Un repetidor es un dispositivo de capa física utilizado para interconectar los segmentos de una red extendida. El repeater esencialmente se comporta posibilitando que varios segmentos de cable sean tratados como uno solo. Reciben señales de un segmento de red, las amplifican, re temporizan y las retransmiten hacia los demás segmentos. Estas acciones previenen el deterioro de las señales causadas por la longitud del cable y la cantidad de los dispositivos conectados.

Hubs

4.3 Un Hub es un dispositivo de capa física que conecta múltiples estaciones de usuario a través de un cable dedicado. Las conexiones eléctricas se establecen en el interior del Hub. Los Hubs crean una red física estrella, al mismo tiempo que mantienen la configuración lógica en bus o ring de la LAN. Podría decirse que el Hub funciona como un repeater multipuerto.

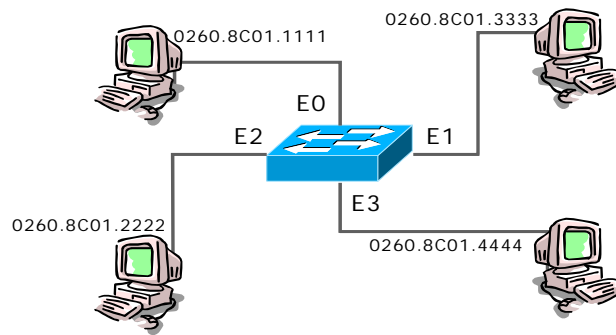
Bridges y Switches

4.4 Los bridges y switches³ son dispositivos que funcionan principalmente en la capa 2 del Modelo de Referencia OSI. (Dispositivos de capa de enlace de datos). Varios tipos de operaciones de bridging han tenido lugar en los escenarios de internetworking. Los bridges transparentes han sido principalmente aplicados en los entornos Ethernet, mientras que los bridges source-route se utilizaron en las redes Token Ring. Los bridges de capa MAC, están diseñados para operan entre redes homogéneas, mientras que otros pueden traducir diferentes protocolos de capa de enlace (por ejemplo IEEE 802.3 e IEEE 802.5).



4.5 Actualmente la tecnología de conmutación (switching) ha emergido como sucesor evolucionario en las soluciones de red. Superior performance, throughput, mayor densidad de puertos, menor costo por port y mayor flexibilidad son las características que contribuyeron al éxito de los switches para reemplazar a los bridges y complementar a los routers.

³ Aclaración: existen switches ATM, LAN switches, y varios tipos de switches de WAN.



4.6 Los switches son significativamente más rápidos que los bridges porque la conmutación se implementa en hardware (existen switches store&forward, cut-through y fragment-free). Pueden interconectar redes Ethernet a 10, 100 y 1000 Mbps.

Full-Dúplex

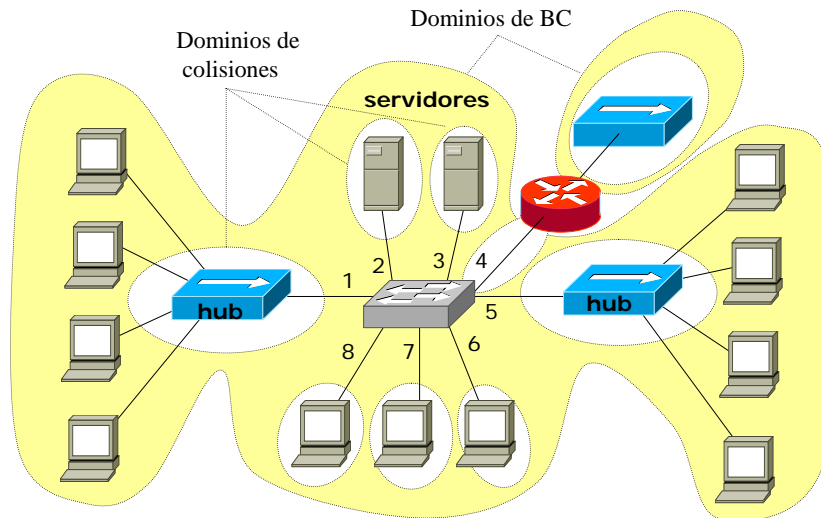
4.7 El comportamiento en Half-Dúplex es requerido cuando las estaciones utilizan un hub Ethernet 10BaseT, el cual recrea un equivalente eléctrico del bus y las reglas CSMA/CD permanecen en efecto. Si la topología permite colisiones, entonces CSMA/CD debe ser utilizado para reaccionar a las mismas.

4.8 La operación Full-Dúplex no es posible con un hub 10BaseT compartido, pero si es posible cuando se quita la posibilidad de que existan colisiones (como en un switch). Esto da origen a las redes switcheadas.

Colisiones y Broadcasts

4.9 Los diferentes dispositivos delimitan los dominios de colisiones y de broadcast.

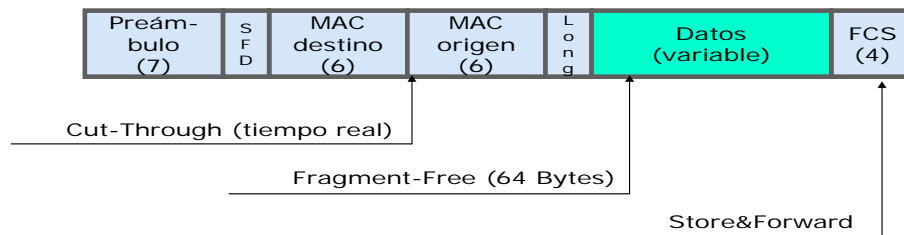
4.10 El **dominio de colisiones** está conformado por todas las placas de red que reciben una transmisión originada en ese dominio (en un hub son todas las interfaces conectadas a sus puertos). Ello provoca que mientras existan señales en el medio de transmisión, todas las otras estaciones deban postergar su chance de transmitir.



4.11 El **dominio de broadcast** esta conformado por todas las interfaces de red que reciben una transmisión broadcast (bc) o multicast (mc) originada en el dominio (un bc trasciende a los hubs, bridges y switches, pero no a un router). En la figura se muestran los dominios de colisiones y de broadcast de una red formada por múltiples dispositivos.

Tipos de operación

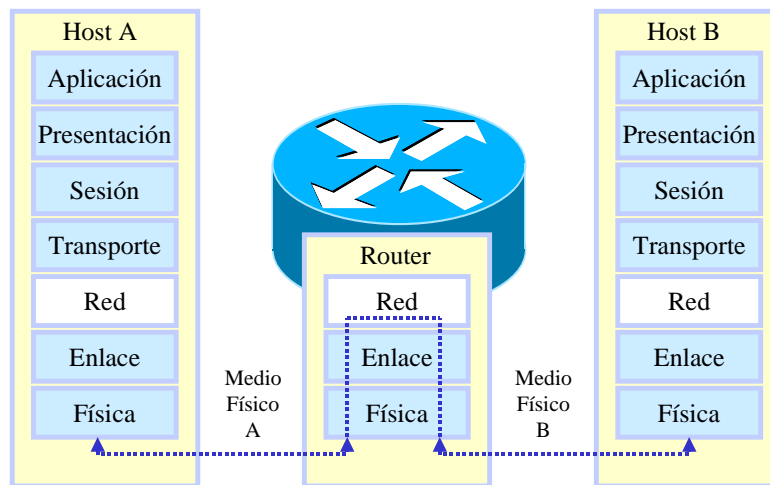
4.12 Entre las ventajas de los switches se encuentra la capacidad de operar en diferentes modos con relación al momento de transmisión de las tramas recibidas. **Store & Forward** es el modo tradicional más lento, en el cual el switch aguarda a recibir el frame completo, para chequear que todos los requisitos de forma están correctos antes de retransmitirlo. El modo **Cut-Through** es el más rápido, ya que una vez determinada la dirección de destino, el frame comienza a transmitirse inmediatamente por el puerto de salida, aunque sin posibilidad de chequear si la unidad reúne los requisitos de longitud, chequeo de errores, etc. Finalmente, el modo Fragment-Free, es un modo intermedio, en el cual el switch aguarda recibir el número mínimo de bits para asegurar que el mismo no constituye un “runt” (frame anormalmente corto, producto de una colisión o error de transmisión).



Routers

4.13 Una de las formas más usuales de interconectar LAN's y subredes en la actualidad es a través del uso de routers. Los routers se instalan en los puntos límites entre dos subredes físicas y/o lógicas. El routing es un método más sofisticado que el bridging para implementar el internetworking. En

teoría, un router (o un conmutador de capa de red) puede oficiar de traductor entre una subred con un protocolo de capa física P1, un protocolo de capa de enlace de datos DL1, y un protocolo de capa de red N1, y otra subred con protocolo de capa física P2, un protocolo de capa de enlace de datos DL2, y un protocolo de capa de red N2. En general, un router se utiliza para interconectar redes que utilizan la misma capa de red, pero diferentes protocolos de capa de enlace.



4.14 Los routers permiten interconectar LAN's a través de WAN's, utilizando los servicios tradicionales (Líneas punto a punto, Frame Relay y ATM), y los nuevos servicios de redes IP/MPLS. Algunos routers operan directamente sobre SDH, y también pueden interconectar LAN's diferentes, tales como Token Ring, y Ethernet.

4.15 La utilización de los routers permite el establecimiento de redes diferentes, tanto física como lógicamente, cada una con su propio espacio de direcciones. Los métodos de enrutamiento se vuelven crecientemente sofisticados, a medida que las topologías crecen en tamaño y complejidad. Los protocolos de capa de red más comunes son IP, IPX, y AppleTalk, aunque la tendencia general está a favor de IP.

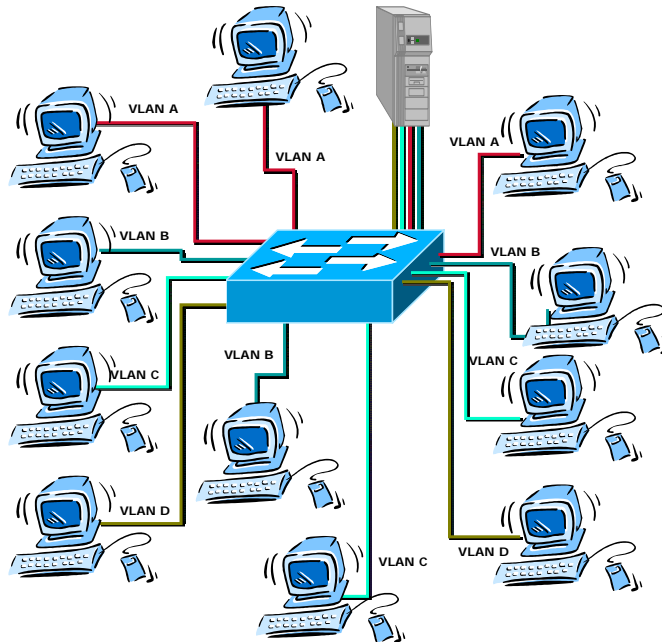
5. VLANs

5.1 Los switches segmentan el dominio de colisiones al máximo (solamente un dispositivo conectado en cada puerto, con la posibilidad de deshabilitar el control de colisiones y transmisión full dúplex). Sin embargo la performance de toda la red es vulnerable al exceso de cierto tipo de tráfico porque los switches propagan los bc y mc hacia todos sus puertos.

5.2 Una forma de limitar el alcance del tráfico mc y bc es a través de la configuración de VLANs (redes LAN virtuales). El soporte de VLAN's permite aislar redes dentro de un mismo switch (también puede extenderse a varios switches), impidiendo que los dispositivos conectados a puertos de VLANs diferentes puedan comunicarse (excepto que se integren a través de un router). El diseño de VLANs está basado en consideraciones de seguridad, performance, administración, etc.

5.3 La figura muestra un switch con soporte de VLANs en el que se han configurado 4 VLANs: A, B, C y D.

5.4 En este ejemplo, cada puerto del switch constituye un dominio de colisiones (en realidad no existirán colisiones, y su detección puede ser desactivada tanto en los dispositivos como en los puertos del switch). La diferencia substancial respecto al esquema del switch sin VLANs es que ahora cada VLAN constituye un dominio de broadcast (es decir que un bc o mc transmitido en la VLAN 2, por ejemplo, no será trasladado a las otras 3 VLANs).



5.5 Todas las terminales conectadas a los puertos pertenecientes a una misma VLAN podrán comunicarse, pero no podrán hacerlo con aquellas conectadas a VLANs diferentes.

5.6 Para posibilitar que todas las terminales puedan acceder al servidor, existen dos posibilidades:

5.6.1 Utilizar cuatro puertos del switch, cada uno perteneciente a una VLAN y conectarlos a 4 interfaces Ethernet instaladas en el servidor.

5.6.2 Utilizar una única interface con soporte de un protocolo de trunking (también soportado por el switch) para conectarla al puerto del switch que transporte el tráfico de todas las VLANs.

5.7 En ambos casos, si se habilita la función de routing en el servidor, también será posible que las terminales ubicadas en VLANs diferentes puedan comunicarse entre ellas.

6. REDES Y DISPOSITIVOS WAN

CARACTERÍSTICAS WAN

6.1 Las características más importantes de las WAN son:

6.1.1 Área geográfica extendida: la red opera más allá del campo geográfico local de una LAN y –generalmente- utiliza los servicios de un carrier para interconectar dispositivos sobre áreas globales.

6.1.2 Las WAN utilizan conexiones –interfaces- en serie de diversos tipos y velocidades para acceder al ancho de banda.

6.1.3 Proporcionan conectividad tanto full-time como part-time.

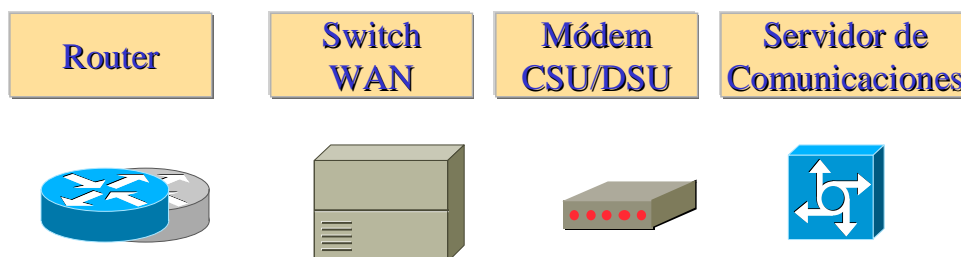
6.1.4 Por definición, una WAN conecta dispositivos separados por áreas amplias. Los dispositivos WAN incluyen:

6.1.4.1 *Routers* que ofrecen múltiples servicios incluyendo internetworking y puertos de interface para WAN.

6.1.4.2 *Switches* que se conectan al ancho de banda WAN para voz, datos y comunicación por video.

6.1.4.3 *Módems* que sirven de interface para servicios de grado de voz. Incluyen unidades de servicio de canal/unidades de servicio de datos (CSU/DSU) que sirven de interface para los servicios T1/E1; adaptadores de terminal/terminación de red (TA/NT), que sirven de interface para los servicios de red digital de servicios integrados (ISDN).

6.1.4.4 *Servidores de comunicaciones* que concentran la comunicación por conexión telefónica para el acceso de usuarios.



6.2 En las redes WAN se utiliza el método de la división en capas OSI para la encapsulación, al igual que las LAN.

TECNOLOGÍAS WAN

6.3 Las especificaciones de capa física de los protocolos WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operativas y funcionales para los servicios de networking de área amplia. Estos servicios, generalmente, se obtienen de proveedores de servicio WAN (carriers).

6.4 Las especificaciones de *enlace de datos* de los protocolos WAN describen cómo se transportan los frames (o tramas) por una única ruta de datos establecida entre sistemas comunicantes. Incluyen protocolos designados para operar a través de servicios dedicados *punto-a-punto*, *multipunto*, y conmutados multiacceso tales como *Frame Relay*.

6.5 Los estándares WAN son definidos y administrados por una cantidad de autoridades reconocidas incluyendo a las siguientes organizaciones:

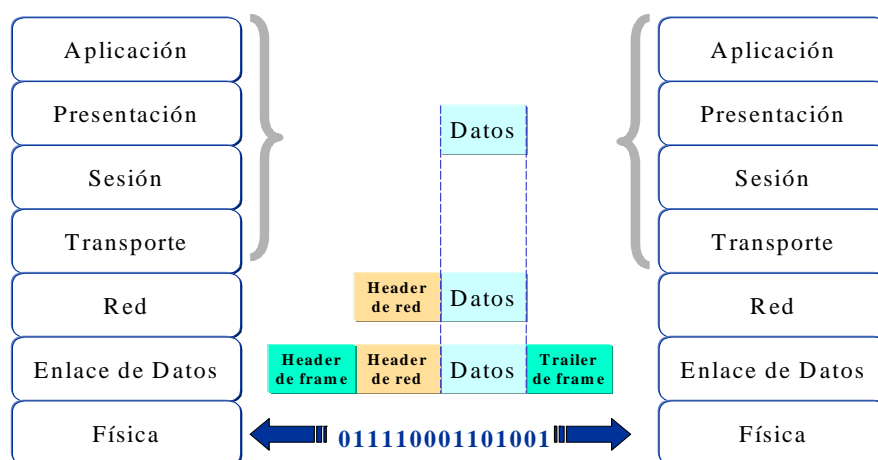
6.5.1 Unión Internacional de las Telecomunicaciones sector de Normalizaciones (ITU-T), ex Comité de Consultoría Internacional para Telefonía y Telegrafía (CCITT)

6.5.2 Organización Internacional para la Normalización (ISO)

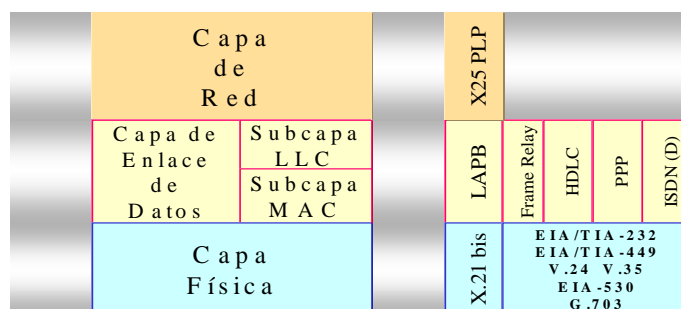
6.5.3 Internet Engineering Task Force (IETF)

6.5.4 Asociación de Industrias Electrónicas (EIA)

6.6 Los estándares y especificaciones de WAN describen tanto los métodos de entrega de la capa física como los requerimientos de la capa de enlace de datos incluyendo el direccionamiento y la encapsulación del flujo de datos. En la figura se muestran las unidades de datos genéricas de los protocolos de las capas inferiores.

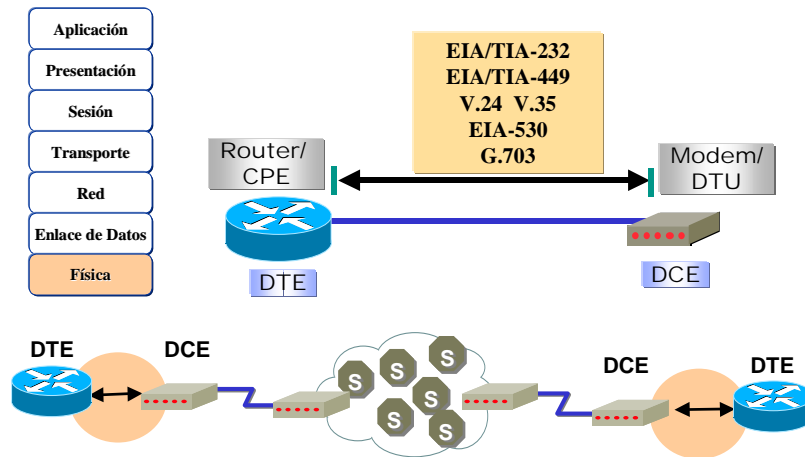


6.7 En la figura siguiente se muestra la pila de protocolos utilizados por las redes WAN.



Capa física

6.8 La capa física WAN describe la interface entre el equipo terminal de datos (DTE) y el equipo de comunicación de datos (DCE). Generalmente, el DCE es el proveedor de servicio, y el DTE el dispositivo conectado. Bajo este modelo, los servicios ofrecidos al DTE se disponen a través de un módem o unidad de servicio de canal/unidad de servicio de datos (CSU/DSU).



6.9 Los siguientes estándares de la capa física especifican estas interfaces:

6.9.1 EIA/TIA-232

6.9.2 EIA/TIA-449

6.9.3 V.24

6.9.4 V.35

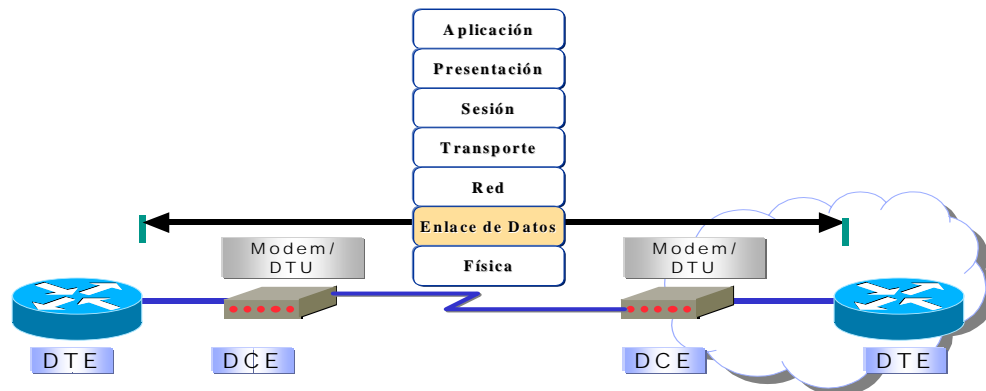
6.9.5 X.21

6.9.6 G.703

6.9.7 EIA-530

Capa de enlace de datos

6.10 A continuación se indican los protocolos de encapsulación de enlace de datos más comunes, asociados con las líneas síncronas en serie.

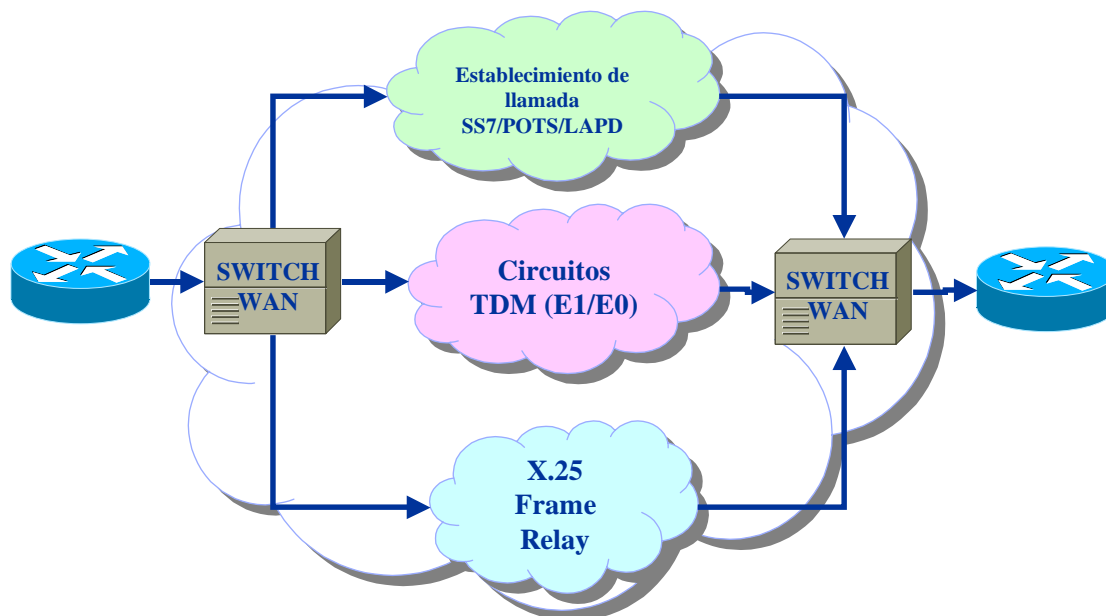


- 6.10.1 **Control de enlace de datos de alto nivel (HDLC)** - Un estándar ISO. HDLC podría no ser compatible entre diferentes fabricantes a causa de la forma en que cada fabricante haya decidido implementarlo. HDLC soporta tanto configuraciones punto a punto como multipunto.
- 6.10.2 **Frame Relay** - Utilizando un entramado simplificado sin mecanismos de control de error a través de facilidades digitales de alta calidad, Frame Relay puede transmitir datos muy rápidamente, en comparación con estos otros protocolos WAN.
- 6.10.3 **Protocolo punto-a-punto (PPP)** - Descrito por RFC 1661, dos estándares desarrollados por la IETF. PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.
- 6.10.4 **Red digital de servicios integrados (ISDN)** - Un conjunto de servicios digitales que transmite voz y datos a través de líneas telefónicas existentes.

7. SERVICIOS WAN

CLASIFICACIÓN DE LOS SERVICIOS

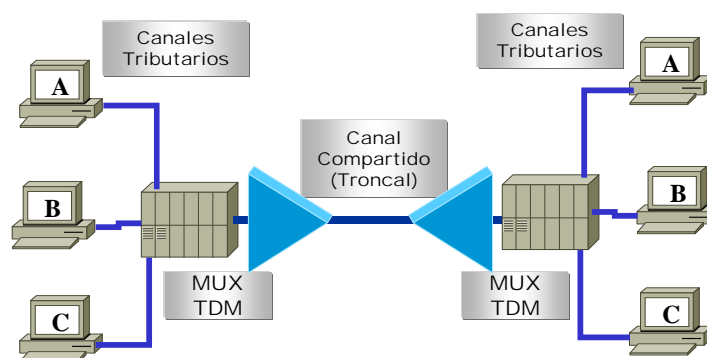
7.1 Como ha quedado expresado, una de las diferencias importantes de las WAN respecto de las LAN consiste en que para las primeras se debe contratar a un proveedor (carrier) para utilizar los recursos de transporte de la red.



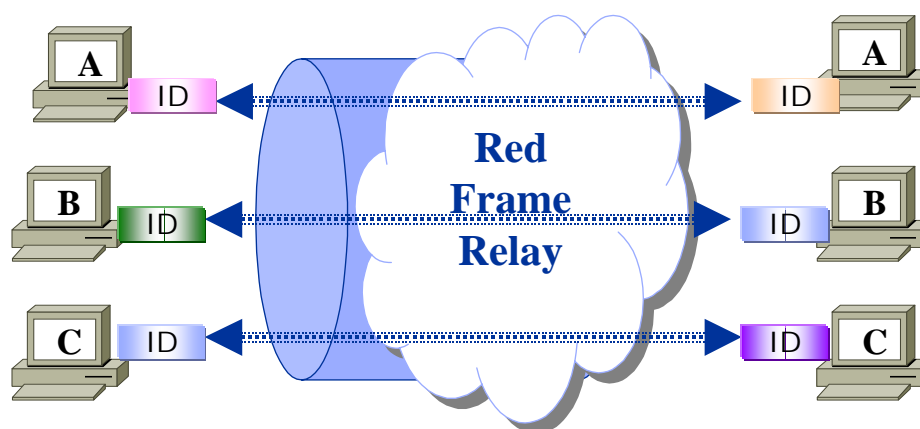
7.2 El servicio telefónico básico es el servicio WAN más comúnmente utilizado. El servicio telefónico y el servicio de datos se conectan desde el punto de presencia (POP) del edificio a la oficina central (CO) del proveedor WAN. Puede establecerse una clasificación preliminar de la “nube WAN”, la cual organiza a los servicios de proveedores WAN en tres tipos principales:

7.2.1 **Servicio de establecimiento de llamada** – Establece y libera las llamadas entre los usuarios telefónicos. El establecimiento de llamada más comúnmente utilizado es señalización por canal común número 7 (SS7). Utiliza mensajes y señales de control telefónico entre los puntos de transferencia a lo largo del camino hacia el destino llamado.

7.2.2 **Multiplexación por división de tiempo (TDM)**—Información proveniente de muchas fuentes posee una ubicación de ancho de banda en un único medio. La conmutación de circuitos utiliza la señalización para determinar la ruta de la llamada, que es una ruta dedicada entre el emisor y el receptor. Con la multiplexación del tráfico en divisiones de tiempo fijas, TDM evita facilidades congestionadas y retrasos variables. El servicio telefónico básico y la red digital de servicios integrados (ISDN) utilizan circuitos TDM.



7.2.3 **Servicios de Conmutación de Paquetes** (tal como X.25 o Frame Relay). La información contenida en paquetes o frames comparte ancho de banda no dedicado con otros frames WAN del suscriptor. La conmutación de paquetes X.25 utiliza enrutamiento de capa 3 con el direccionamiento de emisor y receptor contenidos en el paquete. X.25 puede utilizar circuitos virtuales conmutados (SVCs), con algún retraso inicial para el establecimiento de la llamada, o circuitos virtuales permanentes (PVCs), que evitan los retrasos para el establecimiento de la llamada. Frame Relay utiliza identificadores de capa 2 y circuitos virtuales permanentes (PVCs).



TECNOLOGÍAS

7.3 Existen dos tipos de opciones generales para el networking de área amplia: líneas dedicadas o conexiones conmutadas. Las conexiones conmutadas, a su vez, pueden ser de circuitos conmutados o de paquetes/celdas conmutadas.



7.4 Los enlaces de una red de área amplia pueden ordenarse al proveedor WAN a diversas velocidades que se enuncian en capacidad de bits por segundo (bps). Esta capacidad en bps determinará cuán rápidamente pueden transmitirse los datos a través del enlace.

7.5 El ancho de banda WAN se provee en nuestro medio, Europa y Japón en base a las jerarquías digitales PDH y SDH. El término E1, es el primer nivel de multiplexación de la jerarquía PDH, y se refiere a una señal de 2,048 Mbps.

7.6 Una jerarquía similar se ha desarrollado en los Estados Unidos, donde cada formato se denomina señal digital (DS). El término T1 suele utilizarse coloquialmente para referirse a la señal DS1. El término T3 suele utilizarse para referirse a la señal DS3.

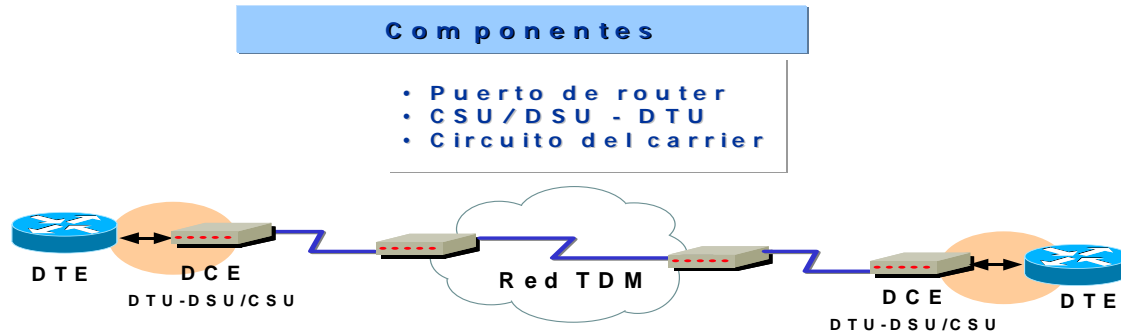
Servicio de líneas dedicadas

7.7 Las líneas dedicadas -o líneas arrendadas- proporcionan un servicio full-time. Las velocidades de transmisión pueden ascender hasta una velocidad E3 (34,364 Mbps), o mayor, pero comúnmente son E1 (2,048 Mbps) o E1 Fraccional (incrementos de 64 kbps o n64Kbps).

7.8 Las líneas dedicadas se utilizan generalmente para transportar datos, voz y video. En el diseño de la red de datos, las líneas arrendadas proporcionan generalmente conectividad principal entre sitios o campus importantes, y conectividad de LAN a LAN.

7.9 Cuando se efectúan conexiones de líneas arrendadas, se requiere un puerto de router para cada conexión, además de una CSU/DSU y el circuito existente del proveedor de servicio.

7.10 El costo de las soluciones de líneas dedicadas puede volverse significativo cuando se lo emplea para conectar muchos sitios, lo cual es especialmente cierto si lo que se desea es emplear una red mallada completa. La conectividad dedicada, full-time, es proporcionada por enlaces en serie punto a punto.



7.11 Las conexiones se efectúan utilizando los puertos seriales sincrónicos del router con un uso típico del ancho de banda de hasta 2 Mbps (E1) disponible a través del uso de una unidad de servicio de canal/unidad de servicio de datos (CSU/DSU). La utilización de diferentes métodos de encapsulación en la capa de enlace de datos proporciona **flexibilidad y fiabilidad** para el tráfico de los usuarios.

7.12 Las líneas arrendadas de este tipo son ideales para ambientes de alto volumen con un patrón de tráfico de velocidad constante. *El uso del ancho de banda disponible es una preocupación puesto que el costo de la línea se paga aún cuando la conexión esté inactiva.*

Servicio de circuitos conmutados

7.13 Las conexiones de circuitos conmutados de un sitio a otro se establecen a la demanda, solamente cuando es necesaria una comunicación y son generalmente de bajo ancho de banda. Las conexiones del servicio telefónico básico se limitan generalmente a 33,6 Kbps. sin compresión, e ISDN a 64 ó 128 Kbps.

7.14 Las conexiones por circuitos conmutados se utilizan principalmente para conectar usuarios remotos y móviles a LANs corporativas. También se destacan como líneas de respaldo para circuitos primarios de mayor velocidad, tales como Frame Relay y líneas dedicadas.

Enrutamiento por llamada bajo demanda

7.15 El enrutamiento por llamada telefónica bajo demanda (DDR) significa que la conexión se efectúa sólo cuando un tipo de tráfico específico inicia la llamada, o cuando es necesario un enlace de respaldo. Estas llamadas de circuitos conmutados, generalmente, tienen lugar sobre redes ISDN.

7.16 DDR es un sustituto ideal para las líneas arrendadas cuando no se requiere la disponibilidad full-time del circuito, como en los siguientes casos:

7.16.1 Cuando los patrones de tráfico son de bajo volumen o periódicos. Las llamadas tienen lugar y las conexiones se establecen sólo cuando el router detecta tráfico marcado como "interesante". Debe evitarse que los broadcasts periódicos, tales como las actualizaciones de protocolo de enrutamiento, disparen llamadas.

7.16.2 Cuando es necesaria una conexión de respaldo para redundancia o carga compartida. El DDR puede utilizarse para proporcionar carga compartida y/o interface de respaldo. Por ejemplo, se pueden tener varias líneas en serie, pero sólo se desea utilizar la línea secundaria cuando la primaria se encuentre muy ocupada, de modo de compartir la carga. Cuando las líneas WAN se utilizan para aplicaciones críticas, pueden configurarse líneas DDR secundarias –de habilitación automática- como backup, en caso de que las líneas principales queden fuera de servicio.



ISDN

7.17 ISDN fue desarrollada por las compañías telefónicas con la intención de crear una red totalmente digital.

Generalidades

7.18 ISDN incluye a los siguientes dispositivos:

7.18.1 **Equipo terminal 1 (TE1)** — Designa a un dispositivo que es compatible con la red ISDN. Un TE1 se conecta a una terminación de red de tipo 1 ó 2 (NT1/NT2).

7.18.2 **Equipo terminal 2 (TE2)** — Designa a un dispositivo que no es compatible con ISDN y requiere un adaptador de terminal (TA).

7.18.3 **Adaptador de terminal (TA)** — Convierte las señales eléctricas estándar a la forma utilizada por ISDN de modo tal que los dispositivos no ISDN puedan conectarse a la red ISDN.

7.18.4 **Terminación de red de tipo 1 (NT1)** — Conecta el cableado del suscriptor ISDN de 4 alambres a la facilidad de bucle local convencional de 2 alambres.

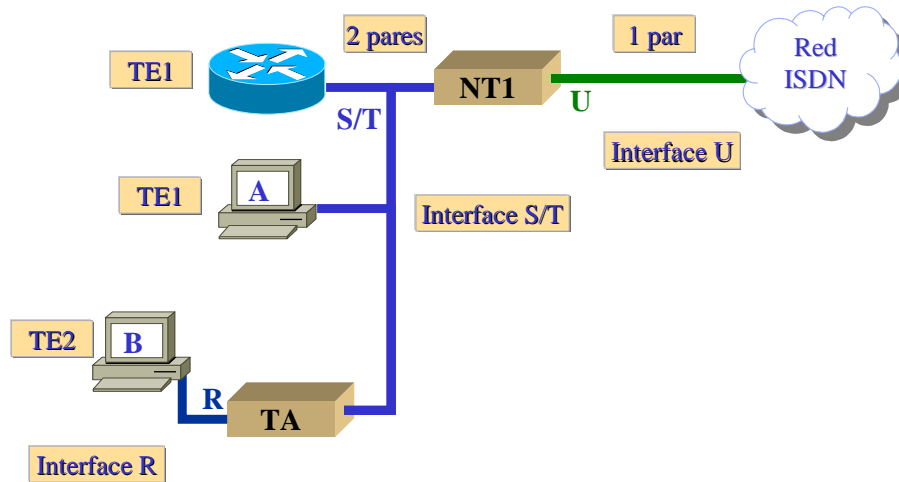
7.18.5 **Terminación de red de tipo 2 (NT2)** — Dirige el tráfico hacia y desde diferentes dispositivos de suscriptor y la NT1. La NT2 es un dispositivo inteligente que efectúa la conmutación y la concentración (por ejemplo una PBX).

7.19 Los puntos de referencia separan a los grupos funcionales de ISDN, y definen los límites de las siguientes interfaces:

7.19.1 La interface S/T define el límite funcional entre un TE1 y el NT. La S/T se utiliza también para definir la interface TA a NT.

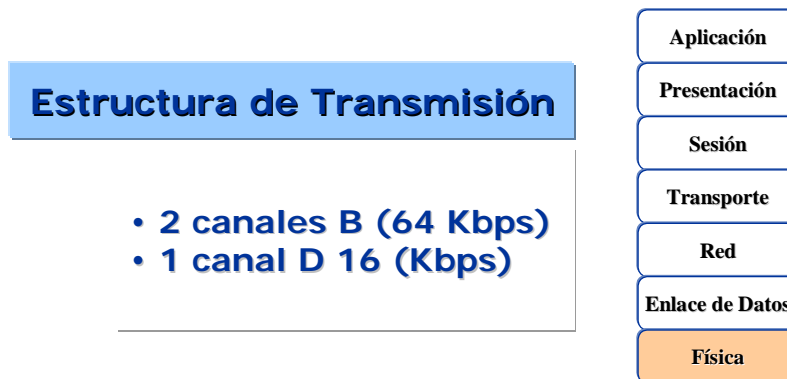
7.19.2 La interface R define a la interface entre un TE2 y el TA.

7.19.3 La interface U define a la interface de 2 alambres entre la NT y la "nube" ISDN.

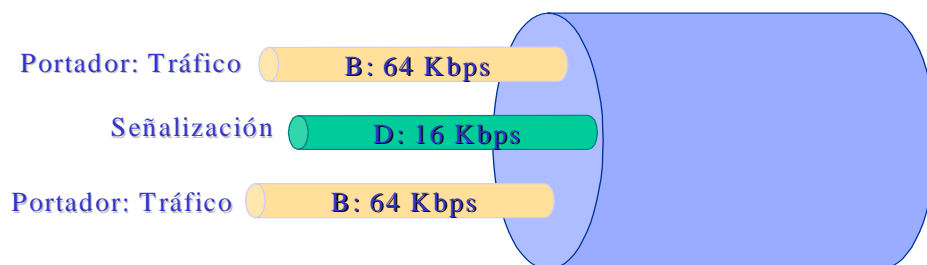


Estructura de transmisión ISDN

7.20 La estructura de transmisión corresponde a la organización de los canales sobre el loop local para acceder a los servicios de soporte. Existen dos estructuras entre el usuario y la central ISDN: la interface de acceso básico (BRI) y la interface de acceso principal (PRI).



7.21 ISDN BRI opera sobre la mayor parte del cableado de cobre correspondiente al plantel exterior telefónico que existe hoy en día, y entrega un ancho de banda total de una línea de 144-kbps en tres canales separados. Dos de los canales, llamados canales B (portadores), operan a 64 kbps y se utilizan para transportar voz o tráfico de datos. El tercer canal, llamado canal D (datos), es un canal de señalización de 16-kbps utilizado para transportar instrucciones que le indican a la red telefónica cómo manejar cada uno de los canales B. ISDN BRI se denomina a menudo "2B+D."

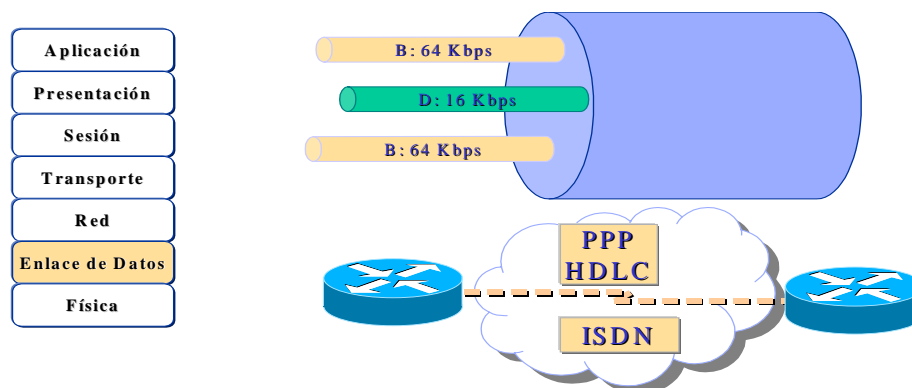


7.22 ISDN provee de una gran flexibilidad al diseñador de red a causa de su capacidad para utilizar cada uno de los canales B para voz o aplicaciones de datos separadas; por ejemplo, un documento

largo podría descargarse de la red corporativa a través de uno de los canales B ISDN de 64-kbps mientras que el otro canal B se está utilizando para examinar una página de la World Wide Web. También podría utilizarse un acceso PRI, con 30 canales B (64 Kbps.) y 1 canal D (64 Kbps.).

Encapsulación de enlace de datos ISDN

7.23 Al emplear soluciones de acceso remoto, están disponibles varias opciones de encapsulación, aunque la de uso más común es el protocolo punto a punto (PPP).



REDES DE CONMUTACIÓN DE PAQUETES

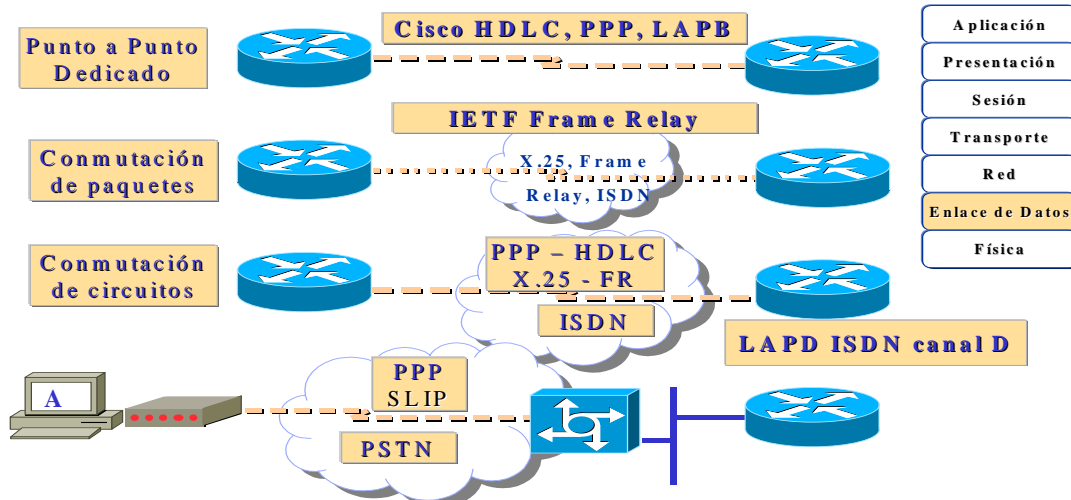
7.24 Las redes conmutadas pueden transportar frames (paquetes) de tamaño variable o celdas de tamaño fijo. El tipo más común de red de paquetes conmutados es Frame Relay. Frame Relay fue diseñada teniendo en mente una velocidad alta y enlaces más fiables. Como resultado, Frame Relay posee una cantidad limitada de características de verificación de errores y fiabilidad. Se espera que los protocolos de capas superiores atiendan estos problemas.

PROTOCOLOS DE ENCAPSULACIÓN WAN

7.25 Cada tipo de conexión WAN utiliza un protocolo de la capa 2 para encapsular⁴ el tráfico mientras éste cruza el enlace WAN. La elección del protocolo de encapsulación depende de la tecnología WAN y el equipo de comunicaciones.

⁴ **Encapsulación** - Envoltura de datos en un encabezado de protocolo particular. Por ejemplo, los datos de Ethernet se envuelven en un encabezado específico de Ethernet antes de su tránsito por la red.

Tunneling - Arquitectura que está destinada a proveer los servicios necesarios para implementar cualquier esquema de encapsulación punto a punto estándar.



7.25.1 **HDLC**—El tipo de encapsulación por defecto de Cisco en enlaces punto a punto. Se utiliza típicamente al comunicarse con otro dispositivo Cisco. Si la comunicación se está efectuando con un dispositivo no Cisco, la opción más viable puede ser PPP síncrono.

7.25.2 **LAPB** (capa 2 del protocolo X.25) – Para las redes de conmutación de paquetes. También puede utilizarse sobre enlaces punto a punto, si el enlace no es fiable o si existe un retraso inherente asociado con el enlace, tal como en el caso de un enlace satelital. LAPB proporciona fiabilidad y control de flujo sobre una base punto a punto.

7.25.3 **PPP**—Común para el acceso por discado telefónico de usuario único a LAN o de LAN a LAN (router a router). PPP está estandarizado, de modo que soporta interoperabilidad entre fabricantes. También soporta la encapsulación de varios protocolos de capa superior incluyendo IP e IPX.

7.25.4 **FR Cisco/IETF**—Utilizado para encapsular tráfico Frame Relay. La opción cisco es propietaria y puede utilizarse sólo entre routers Cisco.

7.26 Se destacan entonces cuatro diferentes métodos de encapsulación de líneas en serie. Aunque presentan características distintas, todas comparten un formato de frame común, como se muestra para HDLC, LAPB y PPP –y en el próximo MD, se realizará para Frame Relay-.



7.27 El frame contiene los siguientes campos:

7.27.1 **Flag**—Indica el principio del frame y se lo determina con el patrón hexadecimal de 7F.

7.27.2 **Dirección**—Un campo de uno o dos bytes para direccionar la estación extrema en ambientes multidrop.

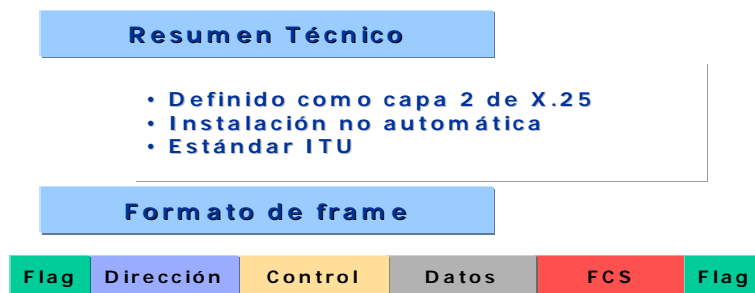
7.27.3 **Control**—Indica si el frame es de tipo de información, de supervisión, o sin numerar. Contiene también códigos de función específicos.

- 7.27.4 **Datos**—Los datos encapsulados.
- 7.27.5 **FCS**— (*Frame check secuencia*) La secuencia de verificación de frames.
- 7.27.6 **Flag**—El identificador de flag 7E de trailer.

ENCAPSULACIÓN HDLC CISCO

7.28 **HDLC**⁵ es el método de encapsulación por defecto de Cisco para líneas en serie. Esta es una implementación muy reducida para su optimización. No hay windowing⁶ o control de flujo⁷, y sólo se permiten conexiones punto a punto (no multipunto).

El campo de dirección siempre se define como todos unos. Además, se inserta un código de tipo propietario de 2 bytes después del campo de control, lo cual significa que el entramado HDLC no es interoperable con equipos de otros fabricantes.



ENCAPSULACIÓN LAPB

- 7.29 LAPB (Link Access Procedure Balanced) es el protocolo estándar de capa 2 definidos por X.25.
- 7.30 Posee dos direcciones que identifican si la trama es un comando o respuesta. No posee campo Tipo.

ENCAPSULACIÓN PPP

- 7.31 El protocolo punto a punto⁸ (PPP) es un método estándar (RFC 1332, 1661) de encapsulación de línea en serie, el cual incluye un campo de tipo protocolo junto con un protocolo de

⁵ **HDLC** - (*High-Level Data Link Control*) Control de enlace de datos de alto nivel. Protocolo de la capa de enlace de datos, orientado a bit y síncrono desarrollado por ISO. Proveniente de SDLC, HDLC especifica un método de encapsulación de datos sobre enlaces en serie síncronos que utilizan caracteres de frame y checksums. Véase también [SDLC](#).

⁶ **Ventana** - Número de octetos que el remitente desea aceptar, o que el transmisor puede enviar sin reconocimiento.

⁷ **Control del flujo** - Técnica utilizada para garantizar que una entidad transmisora, tal como un módem, no sobrecargue a una entidad receptora con datos. Cuando los buffers del dispositivo receptor están llenos, se envía un mensaje al dispositivo transmisor para que suspenda la transmisión hasta que se hayan procesado los datos en los buffers. En redes IBM, esta técnica se llama *pacing*.

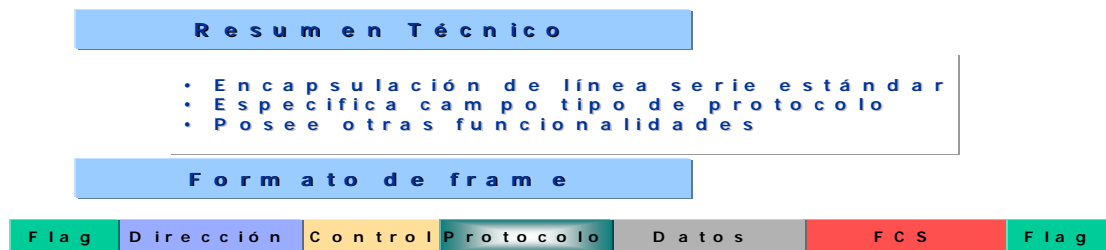
⁸ **PPP** - (*Point-to-Point Protocol*) Protocolo punto a punto. Un sucesor de SLIP, PPP brinda conexiones router a router y host a red sobre circuitos síncronos y asíncronos. Véase también [SLIP](#).

control de enlace. Este protocolo puede, entre otras cosas, verificar la calidad del enlace durante el establecimiento de la conexión.

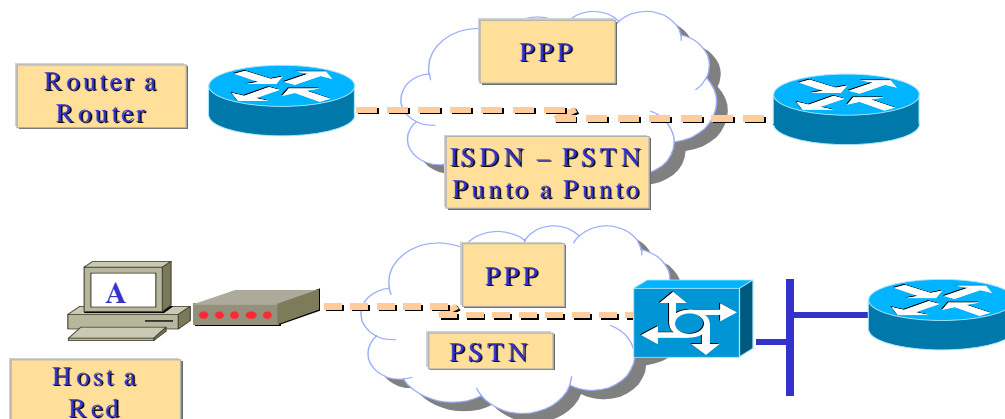
7.32 Además, existe soporte para la autenticación a través del Password Authentication Protocol⁹ (PAP) y el Challenge Handshake Authentication Protocol¹⁰ (CHAP).

7.33 El protocolo punto a punto (PPP) es considerado generalmente como el sucesor del protocolo Serial Line IP (SLIP). PPP proporciona conexiones router a router y host a red a través de circuitos tanto síncronos como asíncronos.

7.34 PPP emergió a finales de la década del '80 en respuesta a una falta de protocolos de encapsulación para la Internet que impedía el crecimiento del acceso en línea en serie. PPP se creó básicamente para



Resolver problemas de conectividad remota a Internet. PPP soporta a diversos protocolos de capa de red, incluyendo a Novell IPX, TCP/IP y AppleTalk.



⁹ **PAP** (*Password Authentication Protocol*) - Protocolo PAP. Protocolo de autenticación que permite a los peers PPP autenticarse unos con otros. Se requiere que el router remoto que intenta conectarse al router envíe una solicitud de autenticación. A diferencia de CHAP, PAP pasa la contraseña y nombre de host o nombre de usuario en la zona libre (no cifrada). PAP no evita por sí mismo el acceso no autorizado, sino que simplemente identifica el extremo remoto. El router o servidor de acceso luego determina si se permite el acceso de ese usuario. PAP es soportado solamente en líneas PPP. Compárese con [CHAP](#).

¹⁰ **CHAP** (*Challenge Handshake Authentication Protocol*) - Característica de seguridad soportada por líneas que utilizan encapsulación PPP que evita el acceso no autorizado. CHAP no evita por sí mismo el acceso no autorizado, simplemente identifica el extremo remoto. El router o servidor de acceso determina luego si se le permite el acceso a ese usuario. Compárese con [PAP](#).

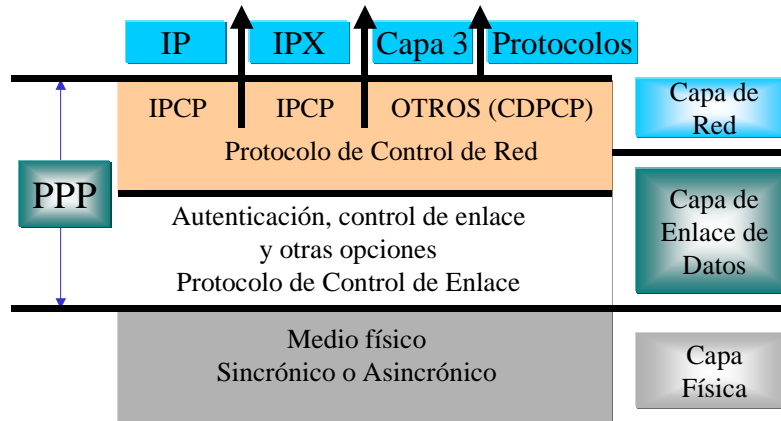
Elementos PPP

7.35 PPP utiliza una arquitectura en capas. Con sus funciones de nivel más bajo, PPP puede utilizar:

7.35.1 Medios físicos sincrónicos tales como los que conectan a ISDN.

7.35.2 Medios físicos asincrónicos tales como los que utiliza el servicio telefónico básico para efectuar conexiones telefónicas vía módem.

7.36 PPP ofrece un rico conjunto de servicios que controlan el establecimiento de un enlace de datos.



7.37 Estos servicios son opciones en LCP y son principalmente la negociación y la verificación de frames para implementar los controles punto a punto que un administrador especifique para la llamada.

7.38 Con sus funciones de nivel más alto, PPP transporta paquetes desde varios protocolos de capa de red en NCPs. Estos son campos funcionales que contienen códigos estandarizados para indicar el tipo de protocolo de capa de red que encapsula PPP.

Operación de PPP

7.39 PPP corre en los siguientes tipos de interfaces físicas WAN:

7.39.1 ISDN

7.39.2 Asincrónica serie

7.39.3 Sincrónica serie

7.40 PPP utiliza otro de sus componentes más importantes, el protocolo de control de enlace (LCP), para negociar y establecer opciones de control en el enlace de datos WAN. PPP utiliza su componente programas de control de la red (NCP) para encapsular diferentes protocolos.

7.41 La transmisión de datagramas PPP emplea tres componentes clave para proporcionar una transmisión de datos efectiva:

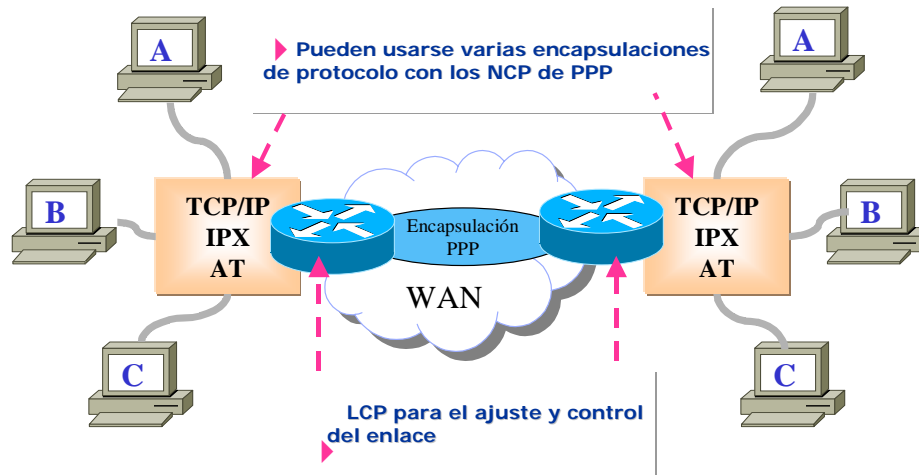
7.41.1 **Encapsulación** - PPP soporta el protocolo de control de enlace de datos de alto nivel (HDLC) para proporcionar encapsulación.

7.41.2 **Protocolo de control de enlace (LCP)** - Se utiliza un LCP extensible para establecer, configurar, y probar la conexión del enlace de datos.

7.41.3 **Protocolos de control de la red (NCP)** - Una familia de NCPs se utiliza para establecer y configurar diferentes protocolos de capa de red.

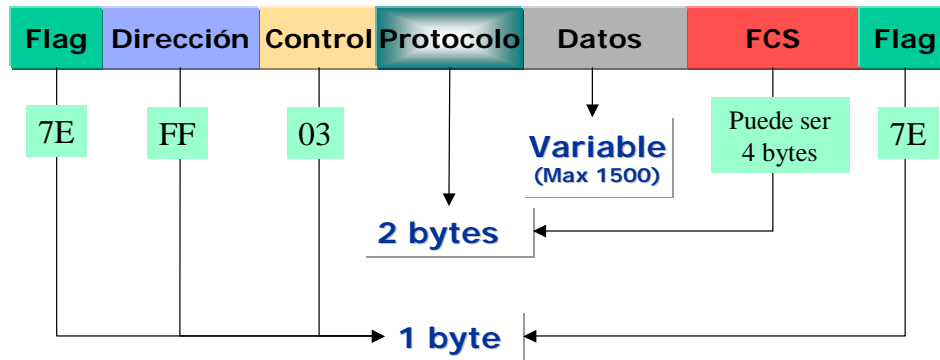
7.42 Las conexiones PPP se establecen en etapas. Un nodo PPP originante envía primero frames LCP para configurar y probar el enlace de datos. A continuación, se establece el enlace, y se negocian las facilidades.

7.43 El nodo PPP originante envía entonces frames NCP para elegir y configurar protocolos de capa de red. Los protocolos de capa de red elegida, tales como TCP/IP, Novell IPX y AppleTalk, se configuran, y se envían los paquetes desde cada protocolo de capa de red.



Formato de frame PPP

7.44 El frame PPP presenta el siguiente formato de campos;



7.44.1 **Flag** - Indica el comienzo o el final de un frame y consiste en la secuencia binaria 01111110.

7.44.2 **Dirección** - Consiste en la dirección de broadcast estándar, secuencia binaria 11111111. PPP no asigna direcciones de estaciones individuales.

7.44.3 **Control** - 1 byte que consiste en la secuencia binaria 00000011, que llama a la transmisión de los datos del usuario en un frame no secuencial. Se proporciona un servicio de enlace sin conexión similar al control de enlace lógico (LLC) tipo 1.

7.44.4 **Protocolo** - 2 bytes que identifican al protocolo encapsulado en el campo de información del frame. Los valores más actualizados del campo de protocolo se especifican en la petición de comentarios (RFC) de los números asignados más recientes.

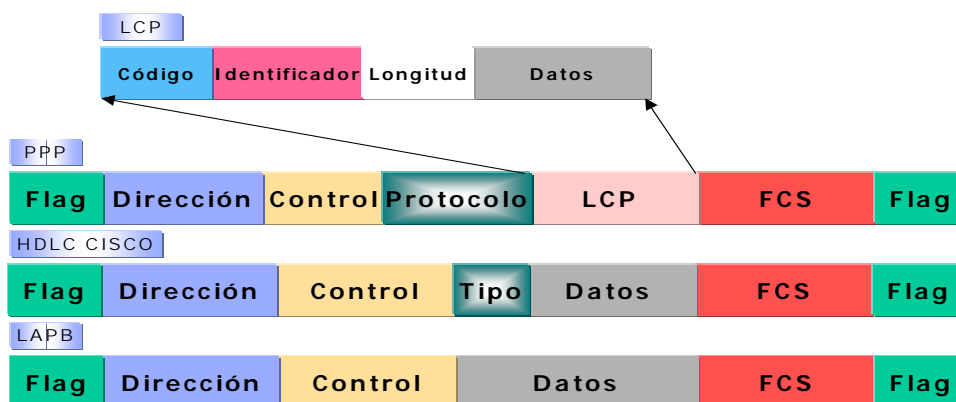
7.44.5 **Datos** - Cero o más bytes que contienen el datagrama para el protocolo especificado en el campo de protocolo. El final del campo información se halla localizando la secuencia del flag de cierre y permitiendo 2 bytes para el campo FCS. La longitud máxima por defecto del campo de información es de 1.500 bytes. Por acuerdo previo, las implementaciones de consentimiento PPP pueden utilizar otros valores para la longitud máxima del campo de información.

7.44.6 **Secuencia de verificación de frames (FCS)** - Normalmente 16 bits (2 bytes). Por acuerdo previo, las implementaciones de consentimiento PPP pueden utilizar una FCS de 32 bits (4 bytes) para una detección de errores perfeccionada.

7.44.7 **Nota** - El protocolo de control de enlace (LCP) PPP puede negociar modificaciones a la estructura de frames PPP estándar. No obstante, los frames modificados serán claramente distinguibles de los frames estándar.

Resumen de Formatos de frames WAN

7.45 El siguiente esquema muestra el resumen de los formatos de frame de los protocolos de encapsulación.



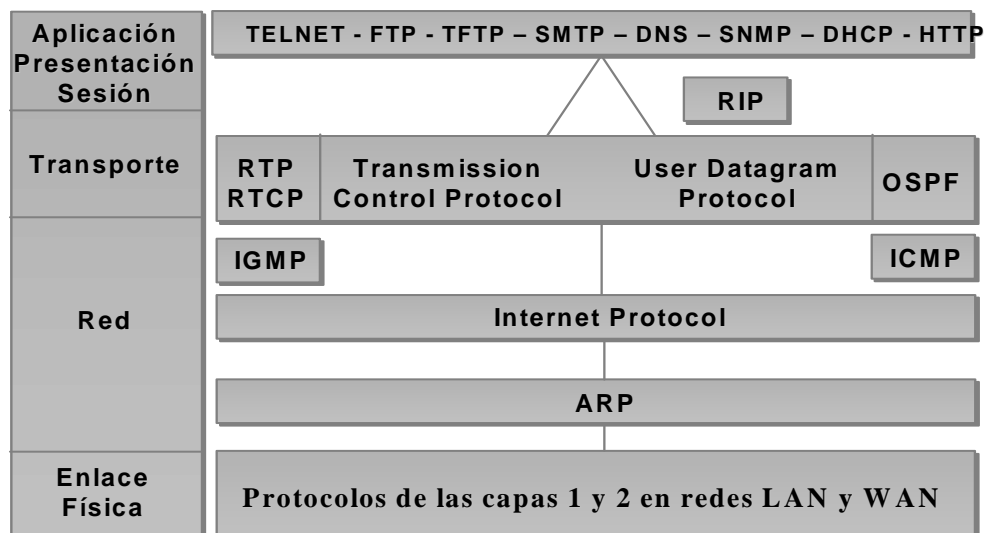
7.46 La siguiente tabla ofrece una síntesis comparativa de los protocolos de enlace de datos más comunes.

Tecnología WAN	Protocolo de Encapsulación	Notas
<ul style="list-style-type: none"> Dedicado Punto a Punto 	<ul style="list-style-type: none"> > HDLC > LAPB > PPP > Frame Relay 	Puede ser cualquier protocolo configurado en ambos extremos.
<ul style="list-style-type: none"> Conmutación de Paquetes 	<ul style="list-style-type: none"> > Frame Relay > X.25 > ATM 	Debe ser el mismo protocolo de la red del carrier.
<ul style="list-style-type: none"> ISDN 	<ul style="list-style-type: none"> > PPP > X.25 > Frame Relay 	En canal D: LAPD. En canal B: cualquiera (similar al punto a punto).
<ul style="list-style-type: none"> PSTN 	<ul style="list-style-type: none"> > Normalmente PPP > Antiguamente SLIP 	Una vez establecido es un punto a punto. Para acceder a Internet PPP.

8. FUNDAMENTOS DE REDES

8.1 El networking evoluciona para soportar tanto las aplicaciones actuales como las futuras. El modelo de referencia OSI organiza las funciones de la red en siete capas. Sin embargo, el “modelo de referencia TCP/IP” solamente establece 4 capas, las que pueden mapearse sobre el primero.

8.2 Los datos fluyen desde las aplicaciones del usuario de nivel superior hasta los bits de menor nivel que se transmiten a través de los medios de red. Las funciones peer-to-peer utilizan la encapsulación y la desencapsulación en las interfaces de las diferentes capas.



8.3 Las principales características de una LAN son:

8.3.1 La red opera dentro de un edificio o dentro del mismo piso de un edificio (extendiéndose hacia el ámbito metropolitano).

8.3.2 Las LAN proporcionan a los diversos dispositivos conectados (generalmente PC) acceso a medios de gran ancho de banda.

8.3.3 Por definición, la LAN conecta computadoras y servicios sobre un medio común.

8.3.4 Los dispositivos de una LAN incluyen: *Bridges* (conectan los segmentos de la LAN y ayudan a filtrar el tráfico), *Hubs* (concentran la conexión a la LAN y permiten el uso de medios de cobre de par trenzado), *Switches Ethernet* (brindan ancho de banda dedicado full duplex a los segmentos o computadoras) y *Routers* que ofrecen muchos servicios entre los cuales se incluyen internetworking y control de broadcasts.

8.4 Los protocolos de la **capa física** de las WAN describen cómo suministrar conexiones eléctricas, mecánicas, operacionales y funcionales para los servicios de WAN. Estos servicios a menudo se obtienen de proveedores de servicios de WAN (carriers).

8.5 Los protocolos de **enlace de datos** de las WAN describen cómo se transportan las tramas entre sistemas a través de un solo enlace de datos. Incluyen protocolos diseñados para operar a través de servicios conmutados dedicados punto a punto, multipunto y multiacceso, como Frame Relay.

8.6 Los estándares de las WAN han sido definidos y administrados por diferentes autoridades reconocidas, tales como las siguientes:

8.6.1 Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), antiguamente denominado Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).

8.6.2 Organización Internacional de Normalización (ISO).

8.6.3 Fuerza de Tareas de Ingeniería de Internet (IETF).

8.6.4 Asociación de Industrias Electrónicas (EIA).

8.7 Normalmente los estándares de WAN describen los requisitos de la capa física y de la capa de enlace de datos (y a veces de red). La capa física de las WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE). Normalmente el DCE es el proveedor del servicio, mientras que el DTE es el dispositivo conectado. En este modelo, los servicios ofrecidos al DTE están disponibles a través de un módem o CSU/DSU.

8.8 En la siguiente figura se observa la relación de los protocolos de las capas 1 y 2, en redes LAN y WAN:

OSI	LAN				WAN			
Enlace	Ethernet	802.2 LLC			HDLC	PPP	LAP B	SDL C
Física		802.3	802.5	FDDI	V.24 – EIA/TIA232 – G703 V.35 - EIA/TIA449 - HSSI			

8.8.1 **Control de Enlace de Datos de Alto Nivel (HDLC):** un estándar IEEE que probablemente no sea compatible con los distintos proveedores, ya que cada proveedor puede haberlo implementado de diferentes maneras. HDLC soporta configuraciones punto a punto y multipunto con un gasto mínimo.

8.8.2 **Frame Relay:** Usa instalaciones digitales de alta calidad y entramado simplificado sin mecanismos de corrección de errores, lo que significa que puede enviar información de Capa 2 mucho más rápidamente que otros protocolos de WAN.

8.8.3 **Protocolo Punto a Punto (PPP):** Descrito por RFC 1661. Dos estándares desarrollados por el IETF. Contiene un campo de protocolo para identificar el protocolo de capa de red.

8.8.4 **Protocolo de Control de Enlace de Datos Simple (SDLC):** Protocolo de enlace de datos de WAN diseñado por IBM para los entornos de la Arquitectura de sistemas de red (SNA). Ha sido reemplazado en gran parte por el más versátil HDLC.

8.8.5 **Protocolo Internet de Enlace Serial (SLIP):** Protocolo de enlace de datos de WAN sumamente popular para transportar paquetes IP. Ha sido reemplazado en varias aplicaciones por el más versátil PPP.

8.8.6 **Procedimiento de Acceso al Enlace Balanceado (LAPB):** Protocolo de enlace de datos utilizado por X.25. Posee amplias capacidades de verificación de errores.

8.8.7 **Procedimiento de Acceso al Enlace en el Canal D (LAPD):** Protocolo de enlace de datos de WAN utilizado para señalización y para la configuración de llamada de Canal D de RDSI. Las transmisiones de datos tienen lugar en los canales B de RDSI.

8.8.8 **Trama de Procedimiento de Acceso a Enlaces (LAPF):** Para Servicios de Portadora en Modo de Trama, un protocolo de enlace de datos de WAN, similar a LAPD, utilizado con tecnologías Frame Relay.

9. PROTOCOLO IP (RFC791-RFC760)

9.1 IP (Internet Protocol) es un protocolo situado en la capa 3 (red) del modelo OSI, diseñado para interconectar redes de comunicaciones por conmutación de paquetes, para formar una internet ó inter-red.

9.2 Se transmiten bloques de datos denominados datagramas, desde una computadora origen, hasta una computadora de destino.

9.3 Cada datagrama contiene información de direccionamiento y de control para enrutar los paquetes, proveyéndose un *servicio de entrega sin conexión* (no se establece una conexión previa a la transferencia de información), de mejor esfuerzo, entre el origen y el destino.

9.4 El dispositivo encargado de encaminar los datagramas entre redes con diferentes esquemas de direcciones se denomina *router*. El router es básicamente un administrador de tráfico (dígame adónde quiere ir, y el router le indicará el camino adecuado).

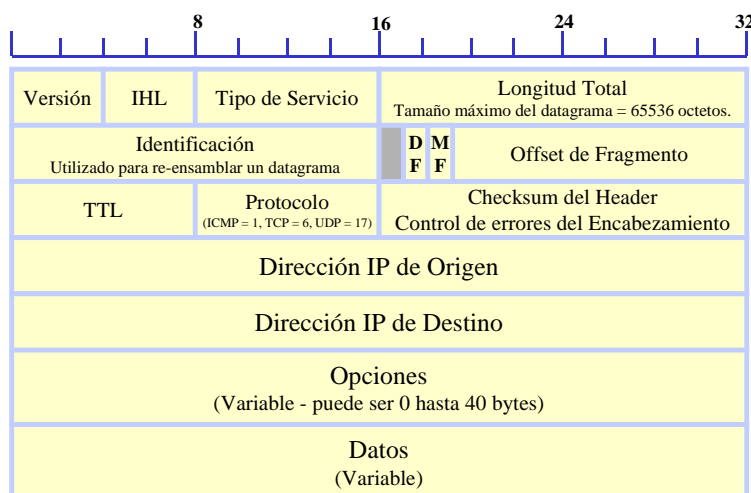
9.5 Los routers poseen puertos, los cuales son conexiones físicas hacia las redes. A cada uno de estos puertos debe asignársele una dirección local. Si existen varios routers, entonces para posibilitar el encaminamiento de los datagramas, cada uno debe conocer la información configurada en los demás.

9.6 Aunque es posible configurar estáticamente todas las direcciones IP y sus puertos asociados, para cada uno de los routers, ello significaría un consumo de tiempo muy grande, para una tarea ineficiente.

9.7 El método apropiado es utilizar protocolos, específicamente diseñados para distribuir la información de encaminamiento entre los routers, llamados *protocolos de enrutamiento*.

Formato del paquete IP (Versión 4)

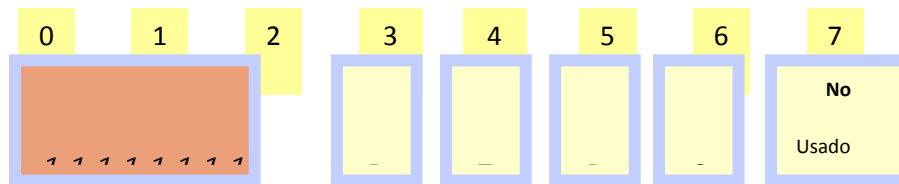
9.8 La siguiente figura muestra el formato del paquete IP versión 4. Los bits se han ordenado de acuerdo con el tratamiento usual de la literatura técnica, es decir en filas de 32 bits (equivalente a 4 octetos).



9.9 **El primer campo, VERS (4 bits, 0 a 3)**, define la versión del paquete IP (actualmente versión 4), con el fin de verificar que emisor, receptor y routers analicen el paquete considerando la versión 4 de la estructura IP, es decir, es el primer parámetro que debe verificarse antes de analizar el mismo ya que en caso de alguna diferencia (entre paquete recibido y software de procesamiento de paquetes) las máquinas rechazarán el paquete para evitar una interpretación incorrecta de su formato.

9.10 **El campo HLEN (4 bits, 4 a 7)**, determina la longitud del encabezado del paquete IP y se expresa en cantidad bytes. Todos los campos de la cabecera tienen una longitud fija, excepto el campo de Opciones IP y Relleno.

9.11 **El Tipo de Servicio**, está a su vez dividido en 5 subcampos de la siguiente forma:



9.11.1 **Prioridad** (3 bits): (o precedencia) indica la prioridad del paquete lo cual permite controlar la información que tendrá mas importancia en el reenvío de los datos, por ejemplo, en la transmisión de VoIP (Voice over IP), el software de aplicación *marca* el paquete en este campo (con cierto valor) para que los routers le den un tratamiento prioritario con respecto a los paquetes de datos.

9.11.2 **D** (1 bit): determina el tipo de transporte requerido para el paquete. Cuando este bit está activado, indica procesamiento con retardos cortos.

9.11.3 **T** (1 bit): determina el tipo de transporte requerido para el paquete. Cuando este bit está activado, indica alta performance.

9.11.4 **R** (1 bit): determina el tipo de transporte requerido para el paquete. Cuando este bit está activado, indica alta confiabilidad.

9.11.5 **Sin Uso** (2 bits).

Por ejemplo, supongamos que un router puede seleccionar entre una línea alquilada de baja velocidad y un enlace satelital de gran ancho de banda (pero con gran retardo) entonces unos paquetes pueden tener activado el bit D y otros tendrán el bit T, en este último caso los paquetes serán reenviados por el enlace satelital. También es muy importante que los algoritmos de ruteo seleccionen la tecnología de red física subyacente que cumpla con las características de bajo retardo, alta performance y alta confiabilidad de manera que en función del estado de estos bits (D, T, R) el algoritmo pueda elegir la interface física que cumpla con el requerimiento definido por el tipo de transporte.

9.12 **El campo Long. Total**, determina la longitud total del paquete IP medido en bytes, por lo tanto como éste tiene una longitud de 16 bits (16 a 31), el tamaño máximo del paquete es de 64 Kbyte ($2^{16}=65.536$).

9.13 **Control de Fragmentación:** Los campos de Identificación, Bandera y Desplazamiento de Fragmentos constituyen los campos que controlan la fragmentación de un datagrama cuando se transmite sobre una red con MTU (Message Transfer Unit)¹¹ menor al tamaño máximo de un datagrama IP.

¹¹ MTU (RFC 1191): NetBios: 512; X.25: 576;; 802.3/802.2: 1492; Eth 2.0: 1500; PPP: 1500; FDDI: 4352; IEEE802.4: 8166; 16M TR: 17914; EtherChannel: 65535

9.14 **El campo de Identificación** determina aquellos fragmentos que son parte de un mismo datagrama original, por lo tanto todos ellos tendrán el mismo valor en dicho campo para que el receptor “entienda” (analizando además la dirección IP origen) que son fragmentos de un mismo paquete.

9.15 **Los campos Bandera y Desplazamientos de Bandera** determinan el orden en el cual deben reensamblarse estos fragmentos. El bit menos significativo del campo Bandera determina si existen más fragmentos (cuando su valor está en “0”) y el campo Desplazamiento, expresado en bytes, determina la posición del fragmento dentro del datagrama original.

9.16 **El campo de Tiempo de Vida:** Expresa el tiempo de vida del datagrama dentro de la red, por ejemplo, cuando un paquete llega a un router, se activa un timer que contabiliza el tiempo de permanencia del mismo dentro del router por lo tanto cuando éste sale, el equipo decrementa el valor del campo Tiempo de Vida en una cantidad igual al tiempo de permanencia del paquete y cuando este valor llega a cero, automáticamente se descarta el paquete de la red y envía un mensaje de error al destino evitando así el viaje indefinido de los mismos dentro de la red.

9.17 **El campo de PROTOCOLO:** Especifica el protocolo de alto nivel que se utilizó para crear el mensaje que se transporta dentro del área de datos.

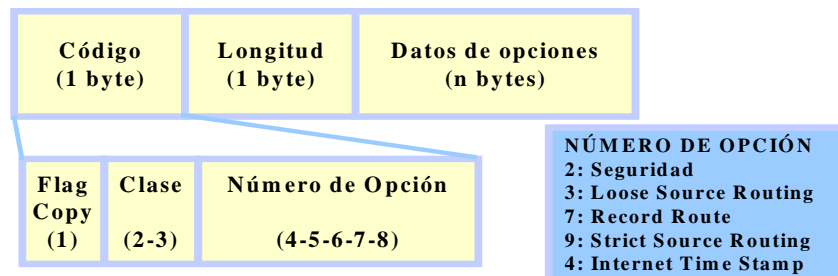
9.18 **El campo Suma de Verificación de Encabezado:** Asegura la integridad de los valores de la cabecera únicamente.

9.19 **Los campos de Dirección Origen y Destino:** Determinan las direcciones de transmisión y recepción del datagrama.

9.20 **El campo de Datos:** Define el área de datos y su longitud es variable.

9.21 **El campo de Relleno:** Depende del contenido del campo Opciones pero pueden usarse para asegurar que la extensión del encabezamiento sea un múltiplo de 32 bits.

9.22 **El campo Opciones:** No está presente en todos los datagramas, y se incluyen en pruebas de red o depuración. Su longitud es variable y dependerá de la opción elegida, por ejemplo, existe un byte dividido en tres partes:



9.23 **Copia:**

9.23.1 1: los routers deben copiar la opción en todos los fragmentos

9.23.2 0: los routers deben copiar la opción en el primer fragmento y no en todos los fragmentos

9.24 **Clase de Opción**

9.24.1 0: Control de red o datagrama

9.24.2 1: Reservado para uso futuro

9.24.3 2: Depuración y mediación

9.24.4 3: Reservado para uso futuro

Clase de opción	Numero de Opción	Longitud	Descripción
0	0	-	Fin de la lista de opciones. Se utiliza si las opciones no terminan al final del encabezado
0	1	-	No operación. Se utiliza alinear octetos en una lista de opciones
0	2	11	Seguridad y restricciones de manejo. Aplicaciones militares
0	3	Var	Ruteo no estricto de fuentes. Se utiliza para rutear un datagrama a través de una trayectoria específica
0	7	Var	Registro de ruta. Se utiliza para registrar el trayecto de una ruta
0	8	4	Identificador de flujo.
0	9	Var	Ruteo estricto de fuente. Se utiliza para establecer la ruta de un datagrama en un trayecto específico
2	4	Var	Sello de tiempo de Internet. Se usa para registrar sellos de hora a lo largo de una ruta

9.25 Las opciones más importantes son las de ruteo y sello de tiempo de Internet porque permite monitorear o controlar la forma en que la red maneja las rutas de los datagramas. La opción de registro de rutas permite a la fuente crear una lista de direcciones IP y arreglar para que cada router que maneja el datagrama añada su propia dirección en cuyo caso el campo Opción tendrá el siguiente formato:

0	7	8	15	16	23	24	31
Código (7)		Longitud (Bytes)			Puntero		
Primera Dirección IP							
Segunda Dirección IP							
...							

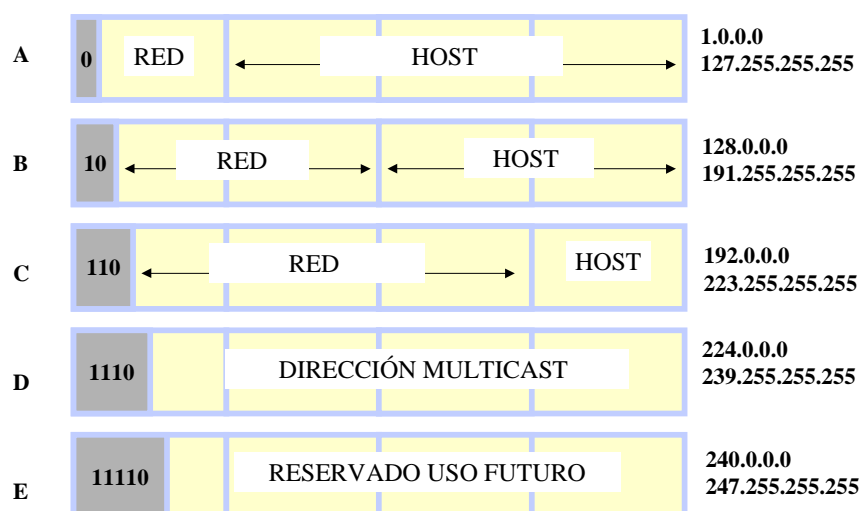
9.26 El campo puntero determina la próxima ranura disponible en la cual el router puede insertar su dirección IP, pero antes de colocar su dirección propia, compara el valor de Longitud (expresado) con el valor de Puntero de manera que si todavía existe “espacio” entonces la incorpora e incrementa el valor del puntero, en caso contrario, enviará el datagrama sin incluirse.

Direcciones IP

9.27 Cada host tiene tantas direcciones IP como puntos de conexión tenga a la red. Existen dos tipos de esquemas de direccionamiento de redes:

9.27.1 **Sin Clase (Classless):** Permite la utilización completa del rango completo de direcciones, sin ningún tipo de reserva de bits para identificar diferentes categorías o clases.

9.27.2 **Con Clase (Classfull):** Esquema de segmentación original (RFC 791) de las direcciones de 32 bits en clases específicas, en las que quedan identificados el número de red y el número de host.



9.28 Los números de red son asignados por el NIC (Network Information Center) para evitar conflictos. En la RFC 1597 se asignan varias direcciones para el uso en redes privadas. Existen protocolos (NAT) para traducir las direcciones privadas (no registradas) a las direcciones públicas y viceversa.

Clase de las Direcciones	Dirección inicial	Dirección final
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Valores especiales

9.29 Si una máquina recibe un paquete cuyo campo Net ID de la dirección destino es igual a cero y el campo Host ID de la dirección destino corresponde a su dirección, entonces el receptor interpreta el campo de Net ID como ésta red. Esta dirección se usa durante el proceso de iniciación, es decir, permite que una máquina se comunique temporalmente y una vez que “aprende” su red y su dirección IP correctas, volverá a utilizar el campo Net ID=0.

9.30 Si una máquina recibe un paquete cuyo campo Host ID de la dirección destino son todos unos corresponde a su dirección, entonces el receptor interpreta el campo de Net ID como ésta red.

9.31 La dirección de red Net ID=127 está reservada para la función de LOOPBACK, es decir, es una dirección de troubleshooting que permite determinar si la pila de protocolos TCP/IP, configurada en la terminal, opera correctamente (ping 127.0.0.1).

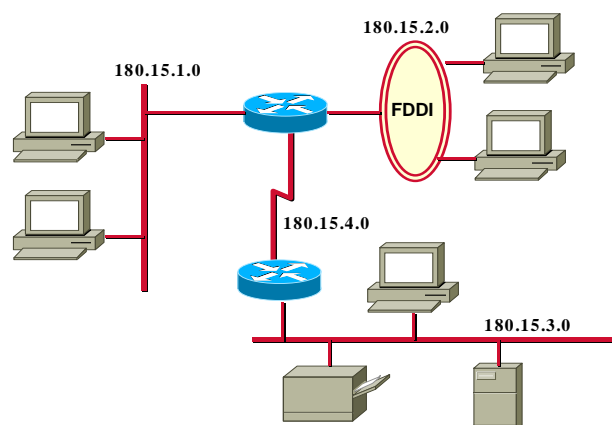
Subdireccionamiento (Subnetting: RFC950)

9.32 Las redes IP pueden ser divididas en redes más pequeñas denominadas subredes. Este procedimiento provee al administrador varios beneficios, incluyendo la flexibilidad, el uso eficiente de las direcciones de red y la capacidad de contener el tráfico broadcast (el broadcast no atraviesa al router). Las subredes se encuentran bajo una administración local, y como tales el resto del mundo ve a la organización como una red única, sin conocer los detalles de la estructura interna.

9.33 Una dirección de red puede ser dividida en varias subredes. Por ejemplo 172.16.1.0, 176.16.2.0, 176.16.3.0, 172.16.4.0, etc., son todas subredes dentro de la red 172.16.0.0 (todos ceros en la parte del número de host de una dirección especifican la red entera).

9.34 Una dirección de subred se crea "robando" bits del campo de host para asignarlos al campo de subred. El número de bits "robado" es variable, y se especifican en la máscara.

9.35 En una organización cuyas direcciones IP no están divididas en subredes, cualquier dirección de la misma se encaminaría en función del valor de su Net ID, por ejemplo, en el caso de la dirección 180.15.0.0 todos los paquetes se encaminarían en base a 180.15 (es un beneficio para el tamaño de las tablas de encaminamiento). Pero tiene el inconveniente que no permite distinguir segmentos individuales dentro de la organización lo cual redundaría en una baja performance de la red, porque todas las terminales "verían" los broadcast de la red.



9.36 El concepto de subdireccionamiento/subnetting/subred facilita una performance más eficiente ya que externamente todo paquete con destino a la organización se encaminará de la misma forma, pero dentro de la organización existen subredes para limitar el tráfico a otros segmentos.

9.37 En el ejemplo, la dirección de red 180.15.0.0 se dividió en 4 subredes: 180.15.1.0, 180.15.2.0, 180.15.3.0 y 180.15.4.0, es decir, en el caso de la dirección 180.15.1.0, 180.15 es la dirección de red, 1 es la dirección de subred y el último campo es la dirección de la terminal de la subred. Desde el punto de vista de la dirección, una subred es una extensión del número de red. Los administradores de red determinarán el tamaño de subred en función de las necesidades.

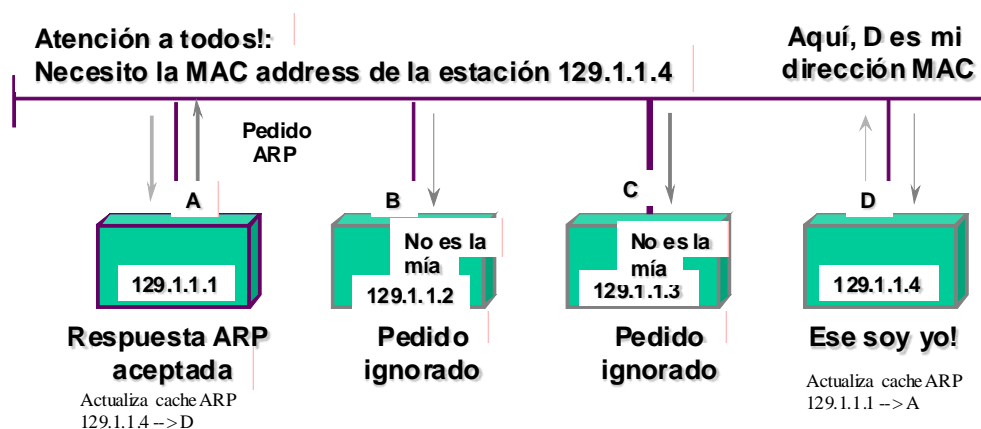
	Red		Host	
	180	15	0	0
Dirección IP	Red		Host	
	255	255	0	0
Máscara Default	Red		Subred	Host
	255	255	255	0
Máscara	Red		Subred	Host
	255	255	255	0

9.38 Los dispositivos usan una "máscara de subred" para determinar la parte de la dirección IP dedicada a la subred. Una "máscara" también tendrá un tamaño de 32 bits, agrupados de 8 como se muestra en la figura.

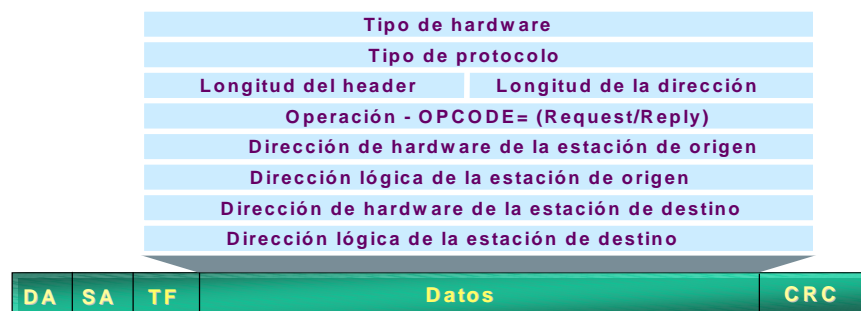
9.39 La forma de calcular la máscara es la siguiente: el campo de red debe ser todos 1's, el campo de subred también deben ser todos 1's y el campo de host deben ser todos 0's, es decir, la máscara de subred indica aquellos bits del campo de host ID, usados para identificar la subred.

ARP (Address Resolution Protocol – RFC826)

9.40 El protocolo ARP, permite mapear la dirección física de la tarjeta de red con la dirección lógica IP del host para encaminar dentro de una subred (segmento de LAN) en función de la dirección IP. Para ello, deberá establecer una relación unívoca entre la dirección física de red (MAC Address) y la dirección lógica IP de la terminal con la cual quiere comunicarse.



9.41 En la siguiente figura se muestra el formato del paquete ARP:



9.41.1 **Tipo de Hardware:** indica el protocolo IEEE802 de LAN. También indica otro tipo de redes.

9.41.2 **Tipo de Protocolo:** indica que es TCP/IP

9.41.3 **Longitud de la Cabecera:** determina la longitud de la cabecera del protocolo

9.41.4 **Longitud de la dirección lógica:** indica la longitud de la dirección lógica

9.41.5 **Operación:** indica si es una interrogación o una respuesta

9.41.6 **Dirección lógica del host transmisor:** indica la dirección lógica del host transmisor

9.41.7 **Dirección física del host transmisor:** dirección física del host transmisor

9.41.8 **Dirección física del host receptor:** dirección física del host destino

9.41.9 **Dirección lógica del host receptor:** indica la dirección lógica del host destino

9.41.10 **TF (Type Field):** determina el tipo de datos que está dentro del paquete: TCP, Apple Talk, XNS

NOTA:

ARP no corre sobre IP, por consiguiente no posee header IP.

Los pedidos ARP son transmitidos en broadcast.

El nuevo EtherType define 0x0806 para los pedidos y respuestas ARP.

Las respuestas ARP se envían directamente a la estación peticionante (unicast, no broadcast).

Las tablas ARP generalmente limitan el tiempo de vigencia de las entradas (age out).

Interface: 168.226.1.203		
Internet Address	Physical Address	Type
168.226.1.1	00-00-0c-03-21-7a	dynamic
168.226.1.6	00-e0-8f-d7-b3-ff	dynamic
168.226.1.43	00-04-00-10-97-cc	dynamic
168.226.1.44	08-00-09-57-53-1e	dynamic

10. TCP¹²

10.1 **TCP (Transmission Control Protocol)** fue específicamente diseñado para proveer un flujo de bytes confiable de extremo a extremo, sobre una interred no confiable. Una interred difiere de una red única porque existen distintas partes de la misma con topologías, anchos de banda, demoras, tamaños de paquetes y otros parámetros sumamente diferentes.

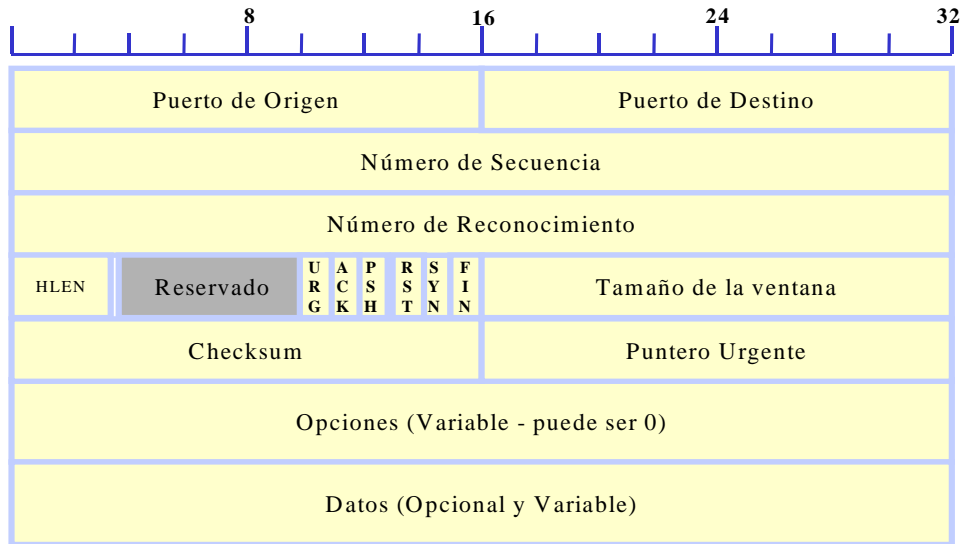
10.2 Cada máquina que soporta TCP debe poseer una entidad de transporte TCP, ya sea en la forma de un proceso de usuario, o parte del kernel que administra los flujos TCP y las interfaces hacia la capa IP.

10.3 Una entidad TCP acepta flujos de datos de los procesos locales, los fragmenta en unidades no mayores de 64 Kbytes (en la práctica unos 1500 bytes), y envía cada parte como un datagrama IP independiente. Cuando los datagramas IP que contienen datos TCP llegan a una máquina, son entregados a la entidad TCP, la cual reconstruye el flujo de bytes original.

10.4 La capa IP no garantiza que los datagramas sean apropiadamente entregados, por ello, es tarea del TCP implementar los mecanismos necesarios para retransmitir, ordenar, reconocer, temporizar, etc. los segmentos, a fin de otorgar la confiabilidad de la transmisión.

10.5 TCP no soporta multicasting, ni tampoco broadcasting.

¹² Las RFC's de TCP son 7 aproximadamente pero las mas importantes son las siguientes: RFC 793; RFC1122: actualización de la anterior (793); RFC 813: administración de ventanas; RFC 816: fallas de aislamiento y recuperación y otras. Las RFC's pueden consultarse en WWW.IETF.ORG



Puertos de origen y destino

10.6 **Los puertos de Origen y Destino:** Identifican los puntos extremos de la conexión. Cada host puede decidir como asignar sus propios puertos, comenzando en 1024. Un port más la dirección IP del host forman un TSAP (Transport Service Access Point) único de 48 bits, también llamado socket. El par de números sockets de origen y destino identifican la conexión.

Socket TSAP	=	Dirección IP	+	Número de Puerto
[48 bits]	=	[32 bits]		[16 bits]

10.7 Los números de puertos desde el 0 hasta 1023 se denominan puertos bien conocidos (well-known ports), y están reservados para servicios estándar (por ejemplo cuando se desea utilizar los servicios FTP, es normal pedir una conexión con el port de destino 21 para contactar al proceso FTP; similarmente Telnet utiliza el port 23). La lista de puertos bien conocidos se brinda en RFC 1700.

Número de secuencia

10.8 **Número de Secuencia y Reconocimiento:** Son los números de segmentos en transmisión y recepción, los cuales implementan el procedimiento usual de la conexión con reconocimiento.

Longitud del header

10.9 **HLEN (Header Length):** Indica la longitud en unidades de 32 bits, que contiene el header TCP, por cuanto el campo de opciones es de longitud variable. Técnicamente el campo indica el comienzo de los datos dentro del segmento (4 bits). Luego aparece un campo de 6 bits no utilizado.

Flags

10.10 A continuación aparecen 6 flags de 1 bit cada uno.

10.10.1 **URG:** Se activa a 1 cuando el puntero de urgencia se encuentra en uso. El puntero de urgencia se utiliza para indicar el desplazamiento en bytes desde el número de secuencia actual, en donde se encuentran los datos urgentes.

10.10.2 **ACK:** Se activa a 1 cuando el número de reconocimiento es válido. Si el valor de ACK es 0, entonces el campo Número de Reconocimiento es ignorado.

10.10.3 **PSH:** Es una forma de indicarle al receptor que entregue los datos a la capa de aplicación inmediatamente, sin ejecutar almacenamiento alguno (generalmente se colocan en un buffer para optimizar la transferencia a la capa superior).

10.10.4 **RST:** Este flag se usa para resetear una conexión que se ha tornado confusa por alguna razón. También se utiliza para rechazar un segmento inválido, o rehusar un intento de abrir una conexión. En general los segmentos con RST=1 representan un problema a resolver.

10.10.5 **SYN:** La activación de este flag se utiliza para establecer conexiones. El pedido de conexión detenta SYN=1 y ACK=0 para indicar que el campo piggyback no está en uso. La réplica a la conexión soporta un reconocimiento, por ello posee SYN=1 y ACK=1. En esencia, el bit SYN se utiliza como Pedido de Conexión y Aceptación de Conexión (el bit ACK se usa para distinguir entre las dos posibilidades).

10.10.6 **FIN:** Es utilizado para liberar una conexión. Indica que el emisor no posee más datos para transmitir. De cualquier manera, después de cerrar una conexión, un proceso puede continuar recibiendo datos indefinidamente. Tanto el segmento SYN como el FIN poseen números de secuencia, para garantizar su procesamiento en el orden correcto.

Valor de ventana

10.11 **Tamaño de Ventana:** Se utiliza para implementar el control de flujo a través de una ventana deslizante de tamaño variable. Indica cuantos bytes pueden ser enviados a partir del byte de reconocimiento. Un tamaño de ventana = 0 indica que se han recibido correctamente todos los bytes hasta el Número de Reconocimiento - 1, pero que por el momento no es posible recibir más datos.

Código de comprobación

10.12 **Checksum:** Control de errores del segmento completo (incluyendo el pseudoheader). El pseudoheader contiene las direcciones IP de las máquinas de origen y destino, el número de protocolo para TCP (=6) y el cómputo en bytes del segmento TCP, incluyendo el header. La inclusión del pseudoheader TCP en el cómputo del checksum ayuda a detectar paquetes erróneamente enviados, pero viola la jerarquía protocolar, ya que las direcciones IP pertenecen a la capa IP, y no a la TCP.

Opciones

10.13 Este campo fue diseñado para proveer una forma de añadir facilidades adicionales no cubiertas en el header regular. La opción más importante es la que permite a cada host especificar la carga máxima del segmento TCP que está dispuesto a aceptar. Durante el proceso de conexión, cada host anuncia su máximo, y analiza el de su contraparte: el más pequeño gana! (si no se utiliza esta opción, el valor asumido es de 536 bytes, por lo que todos los hosts en Internet deben soportar segmentos TCP de 536+20=556 bytes).

10.14 Otra opción importante es la negociación de un factor de ventana propuesta en la RFC 1323, la cual permite desplazar el campo del Tamaño de Ventana hasta 16 bits a la izquierda. Para enlaces con elevado ancho de banda o retardo, o ambos, la ventana de 64 Kbytes es un problema (teniendo en cuenta que a una línea E3 le toma unos 15 milisegundos agotar la ventana completa de 64 Kbytes, y en una fibra transcontinental el tiempo de retardo ida y vuelta es de unos 50 milisegundos, entonces el emisor se encontrará durante el 70% del tiempo esperando por los reconocimientos).

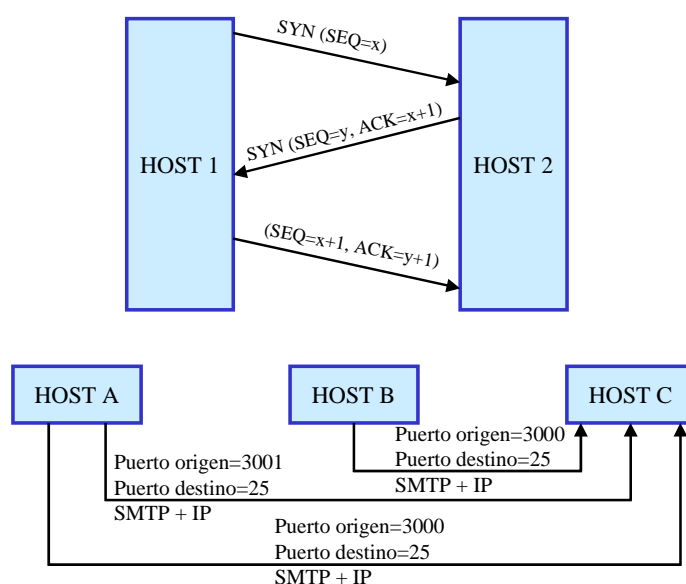
10.15 La RFC 1106 propone la utilización de retransmisión selectiva (NAK), en lugar del protocolo "retroceder hasta N".

Gestión de Conexiones TCP

10.16 Las conexiones en TCP se establecen utilizando un handshaking de tres vías.

10.17 Previamente al pedido de establecimiento, un lado, el server, espera pasivamente el pedido de conexión, ejecutando las primitivas LISTEN y ACCEPT, pudiendo o no indicar una fuente específica.

10.18 El otro lado, el cliente, ejecuta una primitiva CONNECT, especificando la dirección IP y el puerto al cual desea la conexión, el máximo tamaño de segmento TCP dispuesto a aceptar, y opcionalmente algunos datos de usuario (password).



10.19 La primitiva CONNECT envía un segmento TCP con el bit SYN activado, y el bit ACK desactivado, y espera una respuesta. Cuando el segmento llega a su destino, la entidad TCP chequea que algún proceso esté ejecutando un LISTEN en el puerto indicado en el campo Puerto de Destino. Si no es así, envía una réplica con el bit RST=1 para rechazar la conexión.

10.20 Si existe algún proceso "escuchando" en dicho puerto, le es entregado dicho segmento TCP. Éste puede aceptar o rehusar la conexión. Si la acepta, retorna un segmento de reconocimiento (SYN=1, ACK=1)

10.21 A pesar de que las conexiones TCP son full dúplex, es mejor pensar pensarlas como un par de conexiones simplex, a los efectos de entender cabalmente el proceso de liberación. Cada conexión simplex es liberada independientemente de su contraparte. Para ello, cada parte puede enviar un segmento TCP con el bit FIN activado, lo que significa que no existen más datos para transmitir. Cuando dicho segmento es reconocido, ello significa que esa dirección de transferencia ha sido cerrada para el envío de datos, aunque en el otro sentido la transferencia podría continuar indefinidamente.

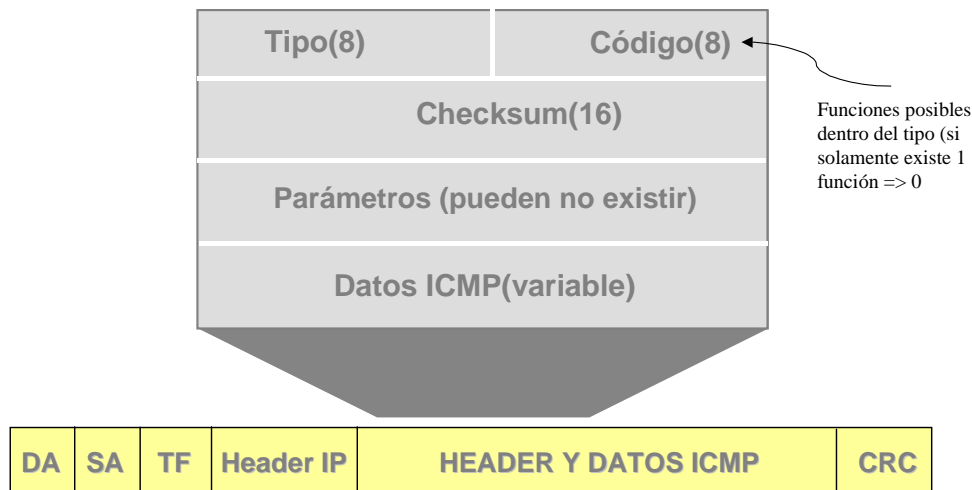
11. ICMP

11.1 Como no existe ninguna provisión por parte de IP para manejar el control de estado y error, ICMP (Mensajes de error y control) es el protocolo que maneja estas instancias para IP.

11.2 Estos mensajes son interpretados por el Protocolo Internet en cada uno de los equipos de red (host/routers).

11.3 Técnicamente el protocolo es un mecanismo de reporte de errores, es decir, permite a los equipos enviar un mensaje a la fuente original cada vez que encuentren un error pero no se especifica del todo la acción a realizar en caso de cierto error.

11.4 Los únicos datagramas que no generan mensajes de error son aquellos que llevan mensajes de error, es decir, si se produce congestión se enviarán mensajes de error los cuales pueden inducir mas congestión pero en este último caso no se generarán mensajes ICMP por lo tanto se evitan los mensajes de los mensajes.



11.5 ICMP no utiliza una capa de transporte -corre directamente sobre IP- por consiguiente es no confiable (no existirán mensajes de error ICMP para un mensaje ICMP. ICMP no pretende convertir a IP en un protocolo confiable, solamente procura reportar errores y proveer feedback ante condiciones específicas.

11.6 El campo Tipo identifica al datagrama ICMP, y el campo Código provee mayor granularidad.

Tipo (8 bits): indica el tipo de mensaje:

- 0: Respuesta de eco
- 3: Destino inaccesible
- 4: Disminución de origen
- 5: Redireccionar (cambiar de ruta)
- 8: Solicitud de eco
- 11: Tiempo excedido para un paquete
- 12: Problemas de parámetros de un paquete
- 13: Solicitud de timestamp

14: Respuesta de Timestamp
15: Solicitud de información
16: Respuesta de información
17: Solicitud de mascara de dirección
18: Respuesta de mascara de dirección

11.7 El campo de código indica posibles funciones dentro de cada tipo (si existe solamente una función, su valor es 0).

Código (8 bit): proporciona más información del tipo de mensajes

0: Red inaccesible
1: Anfitrión inaccesible
2: Protocolo inaccesible
3: Puerto Inaccesible
4: Se necesita fragmentación y configuración DF
5: Falla en la ruta de origen
6: Red de destino desconocida
7: Host de destino desconocido
8: Host de origen aislado
9: Comunicación con la red de destino administrativamente prohibida
10: Comunicación con el host de destino administrativamente prohibida
11: Red inaccesible por el tipo de servicio
12: Host inaccesible por el tipo de servicio

11.8 Por ejemplo el Tipo 3 indica que el host es inalcanzable, pero un código 1 provee una pista más cercana, indicando que el host de destino, y no el port, es inalcanzable (esto podría indicar que aunque se llegó a la red, no hubo ningún host que contestó al ARP REQUEST).

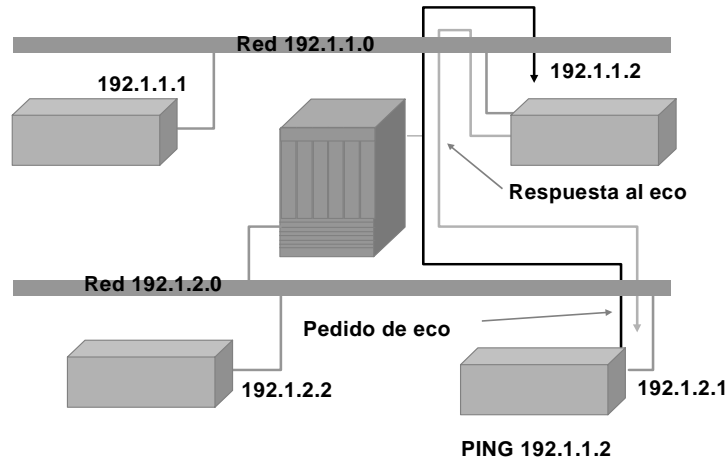
11.9 El checksum computa el complemento a "1" del mensaje ICMP. En los datos se transporta el header y los primeros 64 bits de datos de usuario del datagrama que motivó el mensaje.

ICMP PING

11.10 Uno de los usos más comunes de ICMP es el PING.

11.11 PING se utiliza como herramienta de test y debugging.

11.12 PING es un mensaje ICMP que trata de localizar otras estaciones en Internet para verificar si están activas, o si existe un trayecto habilitado.



12. SWITCHING Y ROUTING

12.1 Existen diferencias y confusiones entre la aplicación rigurosa de los conceptos de bridging, switching y routing y sus implementaciones prácticas.

Switching de capa 2

12.2 El switching (de capa 2) utiliza las direcciones MAC de las tarjetas de interface Ethernet (NIC) para filtrar el tráfico de la red, y está basado en hardware (ASIC). Bridges y switches implementan la función de switching. Como no existen modificaciones en la trama durante el proceso de switching (salvo que se esté bridgeando entre redes heterogéneas, como por ejemplo Ethernet y FDDI), es una operación muy eficiente (bajo costo, alta velocidad y baja latencia).

12.3 Los switches de capa 2 poseen las mismas limitaciones que los bridges (esencialmente están adaptados a los patrones de tráfico locales 80/20). Pero además, aunque segmentan los dominios de colisiones, no pueden quebrar los dominios de bc, pudiendo provocar problemas de performance y limitaciones en el tamaño de las redes. Los mayores inconvenientes que el crecimiento de una red de gran envergadura encuentra con los switches son los bc y mc y la convergencia lenta del protocolo STP (Spanning Tree Protocol).

Bridging:

12.4 El término bridging es completamente análogo al de switching. La diferencia en la aplicación proviene de la elevada densidad de puertos de los switches respecto a los bridges (el switch es como un bridge con múltiples puertos).

Routing

12.5 Los routers no solamente segmentan los dominios de colisiones, sino también los de broadcast. Proveen una determinación óptima de los trayectos porque los routers examinan cada paquete que ingresa a sus interfaces, enviando la información únicamente hacia la red de destino conocida (si el router no conoce la red de destino, el paquete es descartado). La inspección minuciosa de los paquetes es aprovechada para realizar control de tráfico y aplicación de políticas de seguridad. El enrutamiento se realiza en base a las direcciones lógicas de la capa 3 (típicamente IP).

Switching de capa 3

12.6 El switching de capa 3 es funcionalmente similar al routing con todos sus efectos y alcances, sólo que difiere en la forma en la que se implementa en los dispositivos. El switching de capa 3 es un forwarding de paquetes completamente basado en el hardware ASIC.

Switching de capa 4

12.7 El switching de capa 4 es una tecnología similar al switch de capa 3, al que adicionalmente se le han incorporado funciones de enrutamiento relacionadas con las aplicaciones (telnet, FTP, etc.). Es decir que considera los puertos de aplicación de los paquetes para tomar decisiones de enrutamiento.

12.8 La ventaja principal de switching de capa 4 es la posibilidad de implementar calidades de servicio (QOS) basadas en las aplicaciones y usuarios.

Switching de capas múltiples

12.9 El switching de capas múltiples (Multi-layer switching) combina las tecnologías de capas 2, 3 y 4 con características de gran escalabilidad y reducida latencia.

12.10 Un switch multi-layer puede realizar decisiones de switching y routing basándose en:

12.10.1 Las direcciones (MAC) de origen y destino de la trama.

12.10.2 Las direcciones (IP) de origen y destino del paquete.

12.10.3 El campo protocolo del paquete IP.

12.10.4 Los puertos de origen y destino del segmento (TCP o UDP)

DESCRIPCIÓN, COMPONENTES Y OPERACIONES BÁSICAS

DESCRIPCIÓN DEL ROUTER

COMPONENTES DE LA CONFIGURACIÓN INTERNA

CONFIGURACIÓN BÁSICA

MODOS DEL ROUTER

CONFIGURACIONES

PASSWORDS

INICIALIZACIÓN DEL ROUTER

CONFIGURACIÓN DEL ROUTING IP

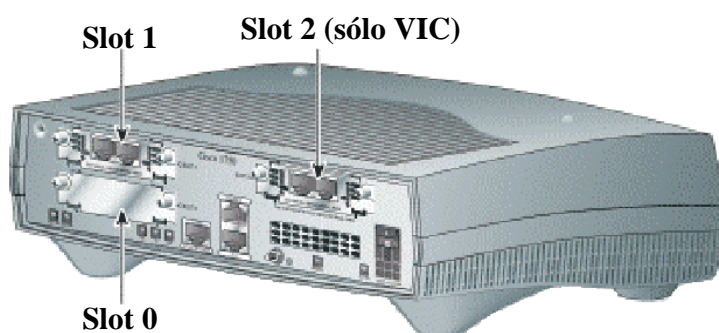
1. DESCRIPCIÓN DE UN ROUTER

1.1 A los efectos de la descripción de los componentes, tomaremos como ejemplo al router Cisco de la línea 1700, el modelo 1751.

Descripción de los componentes básicos

1.2 Los routers de la serie Cisco 1700, proporcionan flexibilidad, seguridad y funcionalidad para las oficinas pequeñas y medianas, al ritmo que evolucionan las redes.

1.3 Para complementar la información, debe consultarse la hoja de datos de la Serie Cisco 1700.¹³



1.4 Los routers de la serie Cisco 1700 conectan las pequeñas oficinas con varias LAN Ethernet a varias WAN a través de conexiones serie síncrona y asíncrona de Red Digital de Servicios Integrados (ISDN).

1.5 El modelo 1751 es un router modular (ofrece tres slots que pueden albergar diferentes módulos de interface). En la figura puede apreciarse la ubicación de los tres slots.

1.6 En la siguiente figura se muestra la parte posterior del router. Dos de los slots han sido ocupados por sendas interfaces de voz FXS.

1.6.1 1 Orificio de bloqueo Kensington.

1.6.2 2 Slot para tarjeta WIC ó VIC (SLOT 1) —Soporta una tarjeta WIC/VIC Cisco.

1.6.3 3 Puerto de consola (azul).

1.6.4 4 Slot para tarjeta VIC (SLOT 2) —Soporta una tarjeta VIC Cisco.

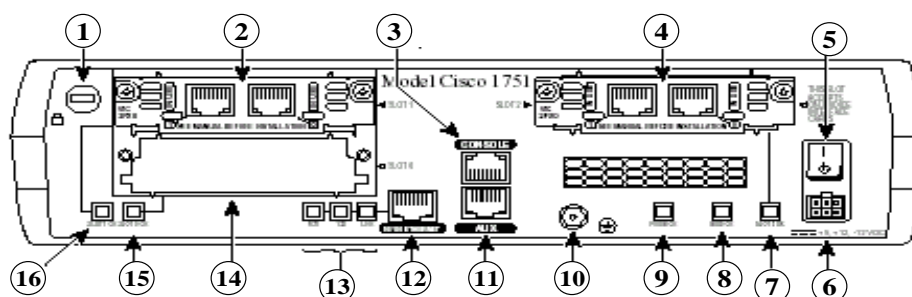
1.6.5 5 Interruptor de energía.

1.6.6 6 Enchufe de energía.

1.6.7 7 LED de estado del Slot 2—On (verde) cuando la VIC esta alojada y funciona correctamente.

¹³ La familia 1700 reemplazo a la familia 1600, a la que se declaró EOS (fin de ventas) y EOL (fin de vida).

1.6.8 **8 LED de estado del MOD—On (verde)** cuando el módulo de encriptación VPN (hardware) está instalado y reconocido por el IOS.



1.6.9 **9 LED de estado del PVDM—On (verde)** cuando el módulo PVDM (hardware interno) está instalado y reconocido por el IOS.

1.6.10 **10 Tornillo de tierra.**

1.6.11 **11 Puerto AUX (negro).**

1.6.12 **12 Puerto 10/100 ETHERNET (amarillo)** —Conecta a la red Ethernet local. Autosensado de velocidad y duplex.

1.6.13 **13 LEDs de la interface Ethernet:**

1.6.13.1 **FDX—ON** indica que el puerto opera en modo full-duplex (**OFF:** modo half-duplex).

1.6.13.2 **100—ON** indica que el puerto opera a 100 Mbps (**OFF:** 10 Mbps.).

1.6.13.3 **LINK—ON** cuando el enlace Ethernet está activo.

1.6.14 **14 Slot para tarjeta WIC ó VIC (SLOT 0)** —Soporta una tarjeta WIC/VIC Cisco.

1.6.15 **15 LED de estado del Slot 0—On (verde)** cuando la WIC ó VIC esta alojada y funciona correctamente.

1.6.16 **16 LED de estado del Slot 1—On (verde)** cuando la WIC ó VIC esta alojada y funciona correctamente.

Interfaces y conexiones del router

1.7 Un router necesita ser configurado para poder operar dentro de una red. Una vez configurado, los administradores de la red, necesitarán verificar el estado de varios de sus componentes.

Puertos de Consola y Auxiliar

1.8 Todos los routers poseen un puerto de consola, el cual es utilizado para acceder al dispositivo en forma directa desde una terminal o una PC con emulación de terminal. Este puerto frecuentemente es una interface RJ-45, denominado “Console”.

1.9 Los cables necesarios los provee Cisco con los siguientes pin-outs:

ROUTER			ROLLOVER		RJ-45 a DB9		
SEÑAL	CONSOLE	AUXILIAR	RJ-45	RJ-45	RJ-45	DB9	SEÑAL
RTS	NO	1 (out)	1	8	8	8	CTS
DTR	2 (out)	2 (out)	2	7	7	6	DSR
TxD	3 (out)	3 (out)	3	6	6	2	RxD
SG	4	4	4	5	5	5	SG
SG	5	5	5	4	4	5	SG
RxD	6 (in)	6 (in)	6	3	3	3	TxD
DSR	7 (in)	7 (in)	7	2	2	4	DTR
CTS	NO	8 (in)	8	1	1	7	RTS

1.10 Después de establecer la conexión física desde la terminal o PC al puerto de consola, es necesario configurar la terminal apropiadamente para posibilitar la comunicación con el dispositivo.

1.11 A continuación, se enciende el router, y podrá visualizarse el banner de arranque. El puerto auxiliar puede ser utilizado para conectar un modem, permitiendo la administración fuera de banda, en caso de pérdida de las otras conexiones. Ambos puertos soportan líneas TTY asincrónicas.

Interfaces

1.12 Son las conexiones a la red, a través de las cuales los paquetes entran y salen del router. Cisco soporta una gran variedad de interfaces, incluyendo Ethernet, Token Ring y seriales. Algunas de las interfaces más comunes del router son seriales (para conexión a enlaces WAN) y LAN (como Ethernet, Token Ring y FDDI).

2. COMPONENTES DE LA CONFIGURACIÓN INTERNA

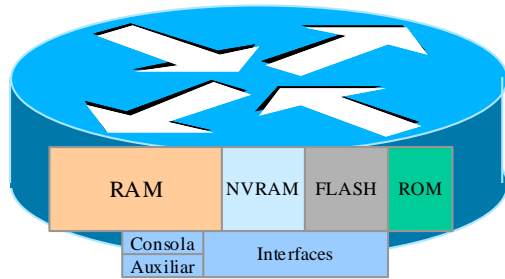
2.1 La arquitectura interna del router (un router es una computadora, y como tal posee elementos de hardware similares a las convencionales) sustenta componentes que juegan un rol muy importante durante el proceso de arranque. Estos componentes son:

2.1.1 Procesador (*CPU*)

2.1.2 *Diferentes tipos de memoria* para almacenar información

2.1.3 Un *sistema operativo* que provee las funciones de operación

2.1.4 *Varios puertos e interfaces* para conectarla a los dispositivos periféricos, o para permitir las comunicaciones con otras computadoras



Elementos del router

2.2 Los componentes de hardware del router incluyen: memoria, procesador, interfaces y líneas.

Memorias

2.3 Existen básicamente 4 diferentes tipos de memoria:

2.3.1 RAM/DRAM

2.3.2 NVRAM

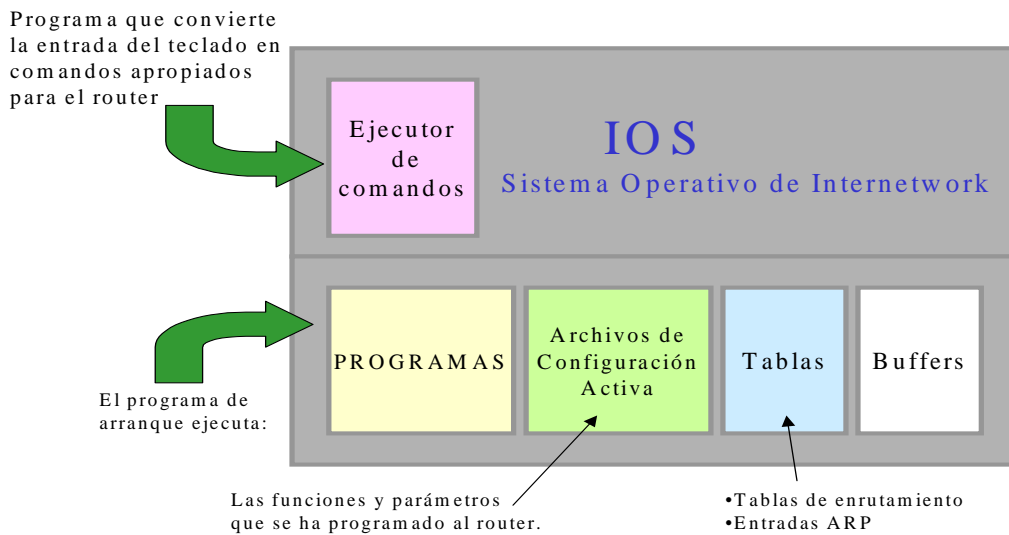
2.3.3 FLASH

2.3.4 ROM

2.4 **RAM/DRAM:** Es el componente de almacenamiento principal para todas las operaciones del router. Se denomina memoria de trabajo y contiene la información de los elementos dinámicos. Parte del IOS también se descomprime en la RAM. Cuando se enciende el router, se ejecuta un programa de bootstrap desde la memoria ROM. Este programa realiza algunas comprobaciones, luego carga el software Cisco IOS en la memoria. El procesador de comandos, o EXEC, es una parte del software Cisco IOS. EXEC recibe y ejecuta los comandos que se ingresan por teclado.

2.5 El router también almacena un archivo de configuración activo y tablas de mapas de redes y listas de direcciones de enrutamiento. Cuando existe una versión de este archivo almacenada en la NVRAM, se accede al archivo guardado y se lo carga en la memoria principal cada vez que se inicia el router. El archivo de configuración contiene información global, de proceso y de interface que afecta directamente la operación del router y de sus puertos de interface.

2.6 La imagen del sistema operativo no puede verse en la pantalla de la terminal. Esta imagen generalmente se ejecuta desde la RAM principal y se carga desde una de varias fuentes de entrada. El software operativo está organizado en "rutinas" que manejan las tareas asociadas a los diferentes protocolos, el movimiento de datos, la gestión de tablas, los buffers, las actualizaciones de enrutamiento y la ejecución de los comandos del usuario.



2.7 **NVRAM:** Este componente es la RAM no volátil (un tipo especial de RAM que no es borrada durante el reboot del router) que contiene una copia de backup de la configuración. Si la energía se pierde, o el router es apagado, la copia de backup de la configuración permite que el router retorne a sus condiciones operativas sin necesidad de una reconfiguración.

2.8 El archivo de la configuración de startup del router es almacenada en la NVRAM, por omisión. Cuando el router sale de fábrica, el archivo de configuración no se halla presente. Este es el primer que se crea durante la configuración. Además guarda el registro de configuración virtual.

2.9 La NVRAM almacena toda la información de configuración del router, definida por el usuario, incluyendo, ente otros: el nombre del host para el router, las tablas de enrutamiento, las configuraciones de protocolos, las configuraciones del caché, y el registro de configuración virtual.

2.10 **FLASH:** Este componente es una clase especial de memoria programable (es como una ROM, pero borrrable y programable, una EEPROM de INTEL). Típicamente la memoria Flash no puede ser modificada durante las operaciones normales del router, pero puede ser actualizada o borrada cuando sea necesario. El contenido de la memoria Flash se mantiene aún después de rebootear el router.

2.11 Esta memoria, normalmente, contiene una copia del software IOS (Cisco Internetwork Operating System). La memoria Flash posee una estructura que admite almacenar copias múltiples del IOS, permitiendo la carga de nuevos niveles del sistema operativo en cada router de la red, y luego, en algún momento conveniente, actualizar toda la red al nuevo nivel.

2.12 La memoria Flash contiene la copia de trabajo del software IOS actual, y es el componente que inicializa el IOS para las operaciones normales del router.

2.13 **ROM:** La memoria de lectura solamente -Read-only memory- almacena el programa de inicialización (**bootstrap**) que permite el arranque básico del hardware del router, y el **POST (power-on self test)**, programas que se utilizan para comprobar la funcionalidad básica del hardware y determinar la presencia de las interfaces.

2.14 La ROM, asimismo contiene el **ROM MONITOR**, un programa monitor de arranque, el cual puede ser utilizado por el administrador para recuperar el sistema ante el evento de una falla de booteo. En algunos routers, la ROM contiene una pequeña versión del software IOS de Cisco, como un backup de emergencia. Los routers Cisco de la serie 7000 and 7500 poseen una versión completa del IOS en ROM.

2.15 En modo ROM monitor el símbolo del prompt es el signo mayor (>).

2.16 Otro componente en la ROM es el Mini-IOS -denominado **RXBOOT** o bootloader- pequeña versión de IOS que puede ser utilizada para activar una interface y cargar un IOS completo en la memoria FLASH, así como otras operaciones de mantenimiento (es como un arranque a prueba de fallos).

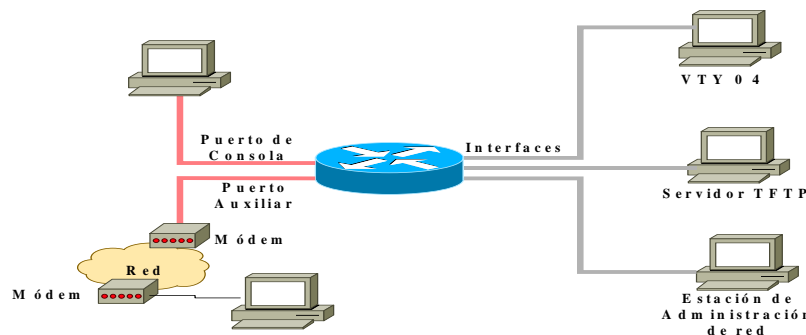
2.17 Los componentes de la ROM no pueden ser modificados durante las operaciones normales del router, pero puede ser actualizado mediante chips de plug-in especiales. El contenido de la ROM se mantiene aún cuando el mismo sea rebooteado.

Fuentes de Configuración

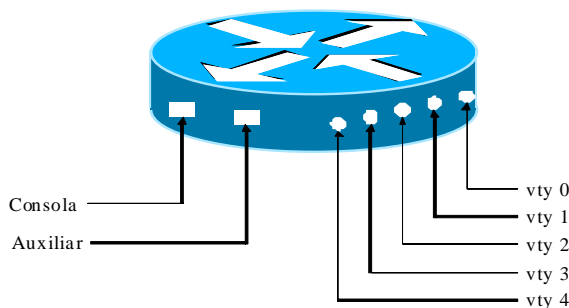
2.18 El router puede configurarse desde diferentes ubicaciones:

2.18.1 En el momento de la instalación inicial, se lo configura desde la terminal de la consola. La terminal de la consola es una computadora conectada al router a través del puerto de la consola. Puede conectárselo por medio de un módem utilizando el puerto auxiliar. Una vez instalado en la red, se lo puede configurar desde las terminales virtuales 0 a 4.

2.18.2 También se pueden descargar archivos desde un servidor TFTP de la red, o gestionarse a través de una aplicación de gestión centralizada.



2.19 La siguiente figura esquematiza los diferentes modos de acceso al router. Las terminales virtuales (vty) son accedidas desde cualquiera de las interfaces para el tráfico normal del router (Ethernet, seriales, TR, etc.).



2.19.1 Los puertos Consola y Auxiliar son puertos físicamente accesibles mediante conectores (EIA-232).

2.19.2 Los puertos denominados VTYx (x= 0, 1, 2, 3 y 4), son virtuales y no existen físicamente, sino que se acceden desde las interfaces que cursan el tráfico normal del router (Ethernet, Serial, TR, ISDN, ATM, etc.), vía el protocolo Telnet. Es decir que debe estar habilitado el protocolo IP.

3. CONFIGURACIÓN BÁSICA

3.1 Una forma de empezar a comprender cómo funciona Internet es configurando un router. Los routers son dispositivos complejos que pueden tener una amplia variedad de configuraciones posibles.

3.2 Después de probar el hardware y cargar la imagen del sistema Cisco IOS, el router encuentra y aplica las instrucciones de configuración. Estas entradas proveen al router detalles de atributos específicos para el router, funciones del protocolo, y direcciones de interface.

3.3 Si el router se halla en una situación de inicio en la cual no puede localizar un archivo de configuración **startup-config** válido, entonces ingresará en un modo inicial de configuración llamado **modo setup**.

MODOS SETUP

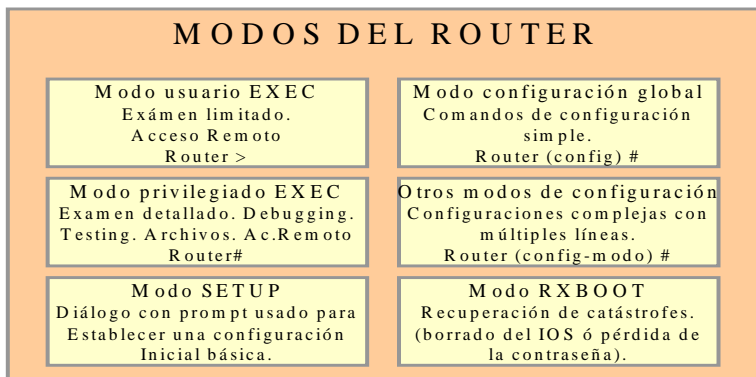
3.4 La rutina para la configuración inicial es el modo **setup**. El propósito principal del modo setup es originar rápidamente una configuración mínima para cualquier router que no puede encontrar su configuración en alguna otra fuente.

3.5 El **setup** no pretende ser el modo de ingresar características complejas del protocolo en el router. Solamente se utiliza setup para una configuración mínima. Es sencillo responder a las preguntas del diálogo de configuración del sistema del comando en modo **setup**, ya que solicita información de configuración básica. Las respuestas permiten al router usar una configuración suficiente, pero de características mínimas, la cual incluirá:

- 3.5.1 Un inventario de interfaces
- 3.5.2 Una oportunidad para ingresar parámetros globales
- 3.5.3 Una oportunidad para ingresar parámetros de interface
- 3.5.4 Una revisión de la información de setup
- 3.5.5 La oportunidad para indicar si quiere que el router use esta configuración

4. MODOS DEL ROUTER

4.1 Ya sea que se acceda desde la consola o mediante una sesión de Telnet a través de un puerto auxiliar, puede colocarse al router en varios modos. Cada modo brinda diferentes funciones:



4.1.1 **Modo de usuario EXEC:** Modo de "sólo mirar" en el cual el usuario puede ver cierta información acerca del router pero no puede modificar nada.

4.1.2 **Modo privilegiado EXEC:** Soporta los comandos de debugging y prueba, el examen detallado del router, la manipulación de archivos de configuración y el acceso a los modos de configuración.

4.1.3 **Modo Setup:** Presenta un diálogo con prompts interactivo en la consola que ayuda a cualquier nuevo usuario a crear una configuración básica de primera vez. Modo de configuración global – Implementa poderosos comandos on-line que realizan tareas simples de configuración. Otros modos de configuración – Brindan configuraciones más complicadas de varias líneas.

4.1.4 **Modo RXBOOT:** Modo de mantenimiento que se puede emplear, entre otras cosas, para recuperar claves perdidas.

4.1.5 **Modos EXEC:** **EXEC interpreta los comandos ingresados y realiza las operaciones correspondientes.**

5. CONFIGURACIONES

5.1 La configuración de los dispositivos de la red determina el comportamiento de la red total.

5.2 Debe procurarse una administración cuidadosa de las configuraciones de los dispositivos: backupearlos, mantenerlos, almacenarlos en servidores de la red para el acceso compartido a los mismos y realizar instalaciones y actualizaciones de software.

Identificación del router

5.3 Una de las primeras tareas básicas consiste en ponerle un nombre al router.

Banners

5.4 Los routers brindan soporte a diferentes tipos de banners que mostrarán información o advertencias a diferentes usuarios en determinadas circunstancias.

5.4.1 Mensaje del día (motd)

5.4.2 Línea

5.4.3 Incoming

5.4.4 Login

Banner EXEC:

5.5 El banner de activación de línea (exec) se muestra cuando se genera un proceso EXEC (tal como una activación de línea o una conexión entrante en una VTY).

Banner incoming

5.6 El banner incoming se muestra en las terminales conectadas en las líneas de Telnet revertido. Muy práctico para proveer información a los usuarios bajo esta modalidad.

Banner login

5.7 Se muestra en todas las terminales conectadas, después del banner MOTD y antes del prompt para el login. El comando activa o desactiva el banner en todas las líneas.

6. PASSWORDS

6.1 Los routers requerirán la configuración de passwords para proteger cuatro accesos:

6.1.1 EXEC privilegiado (ENABLE)

6.1.2 Consola (CONSOLE)

6.1.3 Línea Auxiliar (AUX)

6.1.4 Terminales virtuales (VTY)

6.2 A menos que el router sea configurado para referenciar a un servidor de autenticación externo, las passwords serán almacenadas (en forma explícita o codificada, dependiendo del entorno de seguridad) en el archivo de configuración del router.

Encipción de passwords

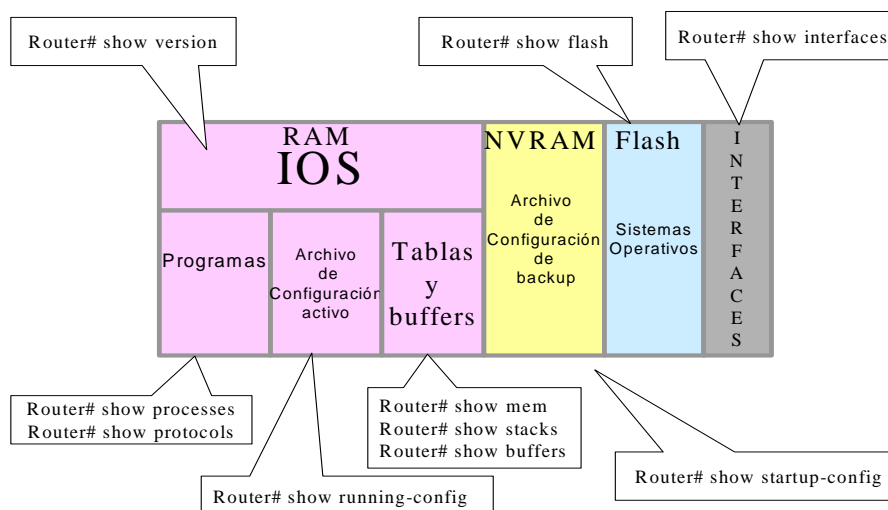
6.3 Cisco ofrece un servicio de encripción de las passwords que normalmente aparecerían en el archivo de configuración en forma explícita (excepto “enable secret”).

6.4 Una vez ingresado el comando, cada password que se configure será almacenada en forma codificada, y no podrá ser recuperada sin un programa de cracking de passwords (muy fácil y ampliamente disponible).

6.5 Cisco utiliza el algoritmo MD5 (no existe forma conocida de revertir este algoritmo) para codificar el “enable secret”. Si se utiliza el “enable secret”, no será posible aplicar las técnicas normales de recuperación de password (salvo por fuerza bruta), las que dependen de visualizar la password en forma explícita en el archivo de configuración, por lo que será menester resetear dicha password.

7. COMANDOS DE ESTADO DEL ROUTER

7.1 En la siguiente figura se muestran los comandos de estado del router:



- 7.1.1 **show versión:** Permite ver en pantalla la configuración de hardware del sistema, la versión de software, los nombres y orígenes de los archivos de configuración y las imágenes de inicio.
- 7.1.2 **show procesos:** Permite ver en pantalla información acerca de los procesos activos.
- 7.1.3 **show protocols:** Permite ver en pantalla los protocolos configurados. Este comando muestra el estado de cualquier protocolo de la capa 3 (la capa de red) configurado.
- 7.1.4 **show mem:** Muestra datos estadísticos acerca de la memoria del router, incluidos datos estadísticos sobre los pools de memoria libre.
- 7.1.5 **show stacks:** Monitorea el uso en pilas de los procesos y rutinas de interrupción y muestra la razón del último reinicio del sistema.
- 7.1.6 **show buffers:** Brinda datos estadísticos sobre los pools de buffer del servidor de la red.
- 7.1.7 **show flash:** Muestra información sobre el dispositivo de memoria flash.
- 7.1.8 **show running-config:** Muestra el archivo de configuración activo.
- 7.1.9 **show startup-config:** Muestra la copia de seguridad del archivo de configuración.
- 7.1.10 **show interfaces:** Muestra datos estadísticos sobre todas las interfaces configuradas en el router.
- 7.2 **Comandos show running-config y show startup-config:** Son quizás los más utilizados de los comandos EXEC del software Cisco IOS, ya que permiten que el administrador vea la configuración actual del router o el tamaño de las imágenes y los comandos de configuración de arranque que utilizará el router la próxima vez que se lo ponga en funcionamiento.
- 7.3 **Comando show interface serial:** El comando show interface serial presenta en la pantalla los parámetros configurables y estadísticas en tiempo real sobre las interfaces serie.
- 7.4 **Comando show versión:** Show version muestra información de la versión del Cisco IOS que ejecuta el router.
- 7.5 **Comando show protocols:** Este comando muestra el estado global y el estado específico de la interface de cualquier protocolo de Nivel 3 configurado (por ejemplo, IP, DECnet, IPX, y AppleTalk).

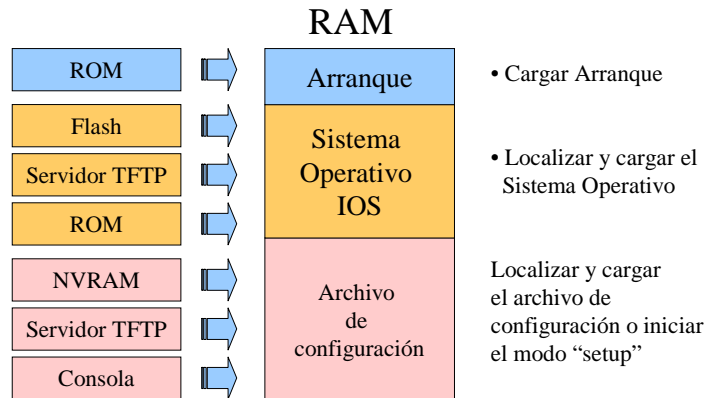
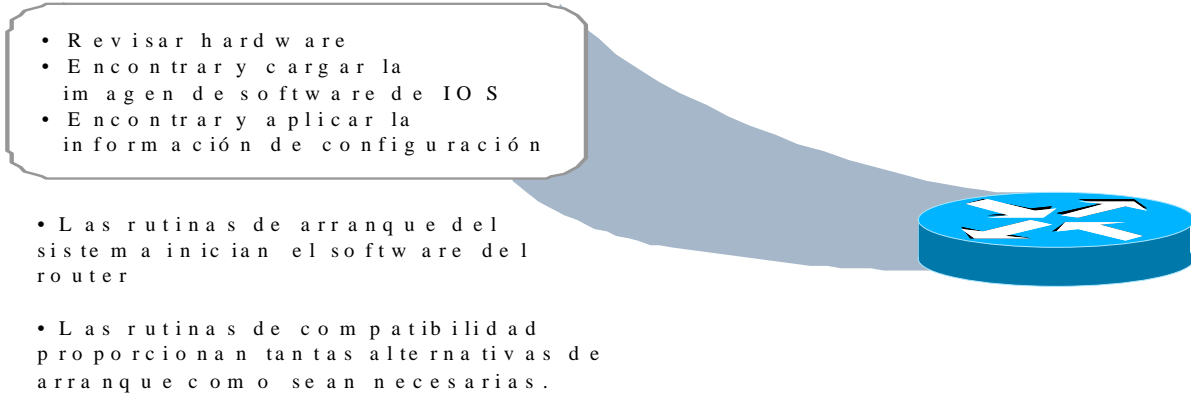
8. INICIALIZACIÓN DEL ROUTER

Rutinas de Arranque

- 8.1 Las rutinas de arranque del software IOS tienen por objeto dar inicio a las operaciones del router. El router debe tener un desempeño confiable en la conexión de las redes de usuario para cuyo servicio fue configurado. Para hacerlo, las rutinas de inicio deben:
- 8.1.1 Asegurarse de que el router tenga todo el hardware probado.
- 8.1.2 Buscar en la memoria y cargar el software IOS que el router utiliza como OS.
- 8.1.3 Buscar en la memoria y aplicar la información de configuración del router, incluidas las funciones del protocolo y las direcciones de las interfaces.
- 8.2 Inmediatamente después del arranque, el router se asegurará de tener el hardware probado, mediante la ejecución de una POST (Power-On-Self-Test).

8.3 La POST, la cual reside y se ejecuta desde la ROM, realiza una auto prueba del sistema, durante la cual, diagnostica todos los componentes. Se verifica la presencia y el funcionamiento básico de la CPU, de la memoria y de los puertos de interface de red.

8.4 Después de verificar las funciones del hardware, el router procede a la inicialización del software.



9. CONFIGURACIÓN DEL ROUTING IP

Tabla inicial de enrutamiento IP

9.1 Inicialmente, el router posee información de las redes o subredes directamente conectadas. Cada interface debe ser configurada con una dirección IP y una máscara. El software IOS debe recibir esta dirección IP e información de máscara desde alguna fuente. La fuente inicial de direccionamiento es la persona que realizar la primera configuración.¹⁴

9.2 Por supuesto, es posible iniciar al router desde una condición de cero -estado que carece de otro origen para una configuración inicial- en modo setup-mode, y responder a los prompts para una información de configuración básica.

¹⁴ El comando global "no ip routing" deshabilita el enrutamiento del protocolo IP.

Información de Rutas

9.3 Los routers conocen las rutas a destinos de tres modos distintos:

9.3.1 **Rutas estáticas:** Definidas manualmente por el administrador del sistema como la única ruta hacia el destino. Son útiles para controlar la seguridad y reducir el tráfico.

9.3.2 **Rutas por defecto:** Definidas manualmente por el administrador del sistema como la ruta a tomar cuando no existe una ruta conocida hacia el destino.

9.3.3 **Enrutamiento dinámico:** El router se entera de las rutas a los destinos al recibir actualizaciones periódicas de otros routers.

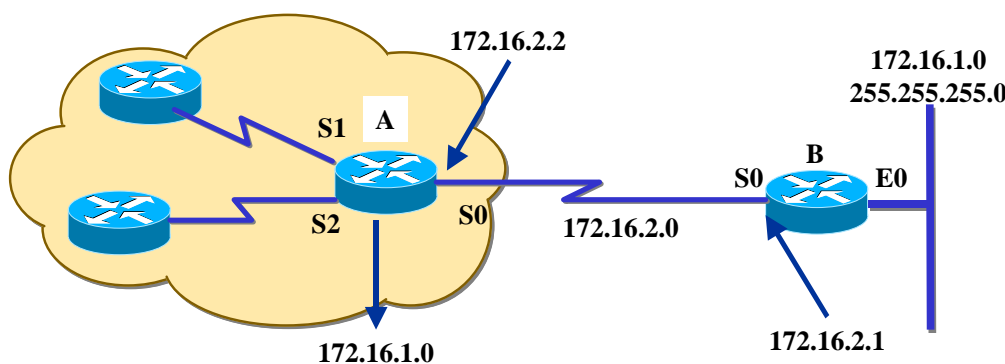
Configuración de rutas estáticas

9.4 Una ruta estática permite una configuración manual de la tabla de enrutamiento. No se producirán cambios dinámicos en una entrada de tabla determinada mientras esté activa la ruta, y en general refleja algún conocimiento especial de la situación de networking conocida para el administrador de red. No se envían actualizaciones de enrutamiento por los enlaces, si sólo se han definido rutas estáticas, conservando el ancho de banda.

9.5 En el ejemplo:

9.5.1 La asignación de una ruta estática para alcanzar la red de conexión única 172.16.1.0 es apropiada para el router A (ISP), porque existe solamente una forma de alcanzar la red del cliente.

9.5.2 La asignación de una ruta estática desde el router B a las redes no visualizadas también es posible. Sin embargo, una asignación de una ruta estática es necesaria para cada red de destino, por lo tanto, una *ruta por defecto puede ser más conveniente*.



```
ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

Comando	Descripción
ip route 172.16.1.0	Especifica una ruta estática a la subred de destino.
255.255.255.0	Una máscara de subred indica que hay 8 bits de conexión en subredes en curso.
172.16.2.1	Dirección IP del router del próximo salto en la ruta al destino.

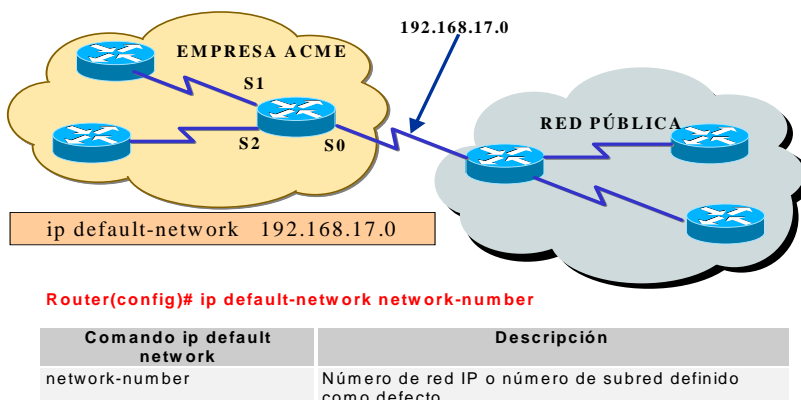
Configuración de rutas por defecto

9.6 Cuando no existe una entrada para la red de destino en la tabla de enrutamiento, el paquete se envía a la red por defecto. La red por defecto debe existir en la tabla de enrutamiento. Las rutas por defecto mantienen la longitud de las tablas de enrutamiento más cortas.

9.7 Debe utilizarse el número de red por defecto cuando se necesite una ruta, de la que solamente se tenga información parcial sobre la red de destino.

9.8 Como el router no tiene un conocimiento completo de todas las redes de destino, puede usar un número de red por defecto para indicar la dirección a tomar para números de redes desconocidas.

9.9 En el ejemplo, el default-network 192.168.17.0 define la red de clase C 192.168.17.0, como la ruta de destino para los paquetes que no tienen una entrada en una tabla de enrutamiento.

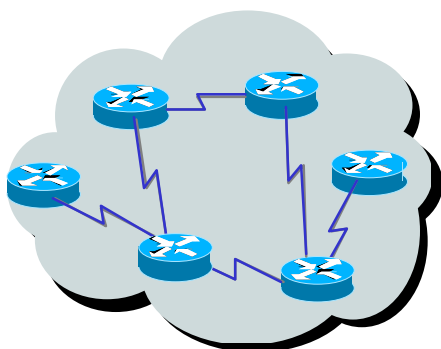


Introducción al enrutamiento dinámico

Sistema autónomo

9.10 En el ejemplo anterior, el Router A podría necesitar un firewall para actualizaciones de enrutamiento. El administrador de la Compañía X no quiere actualizaciones procedentes de la red pública. El Router A puede necesitar un mecanismo para agrupar las redes que compartirán la estrategia de enrutamiento de la Compañía X. Uno de esos mecanismos es un número de sistema autónomo.

9.11 Un sistema autónomo consiste en routers, administrados por uno o más operadores, que presentan una pauta coherente de enrutamiento hacia el mundo externo.

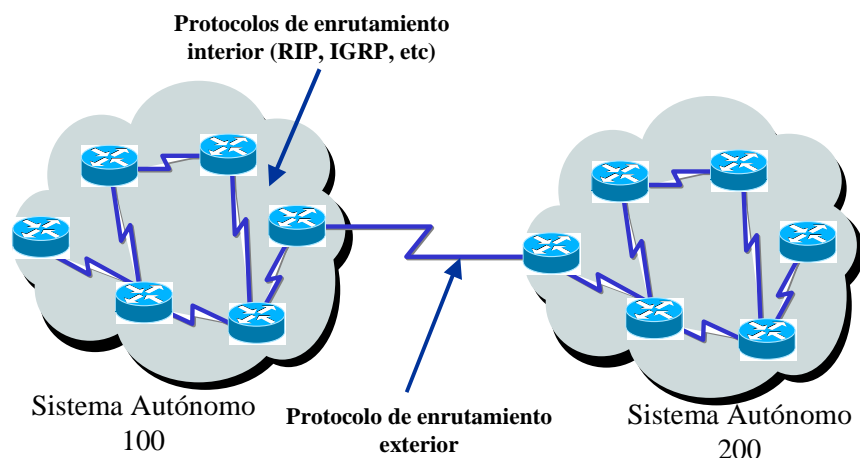


9.12 El Centro de información de la red [Network Information Center] (NIC) asigna un número de sistema autónomo exclusivo para cada empresa. Este sistema autónomo es un número de 16 bits.

9.13 Un protocolo de enrutamiento como el Protocolo de enrutamiento de gateway interior de Cisco [Interior Gateway Routing Protocol] (IGRP) demanda que especifique este número de sistema autónomo exclusivo asignado en su configuración.

Protocolos de enrutamiento interiores o exteriores

9.14 Se utilizan protocolos de enrutamiento exteriores para comunicar entre sistemas autónomos. Se utilizan protocolos de enrutamiento interiores dentro de un único sistema autónomo.



Protocolos de enrutamiento IP interiores

9.15 Los routers pueden utilizar protocolos de enrutamiento -en la capa de Internet del conjunto de protocolos TCP/IP-, mediante la aplicación de algoritmos de enrutamiento específicos.

9.16 Algunos de los ejemplos de protocolos de enrutamiento IP más comunes son:

9.16.1 RIP: Protocolo de enrutamiento por vector de distancia (distance-vector).

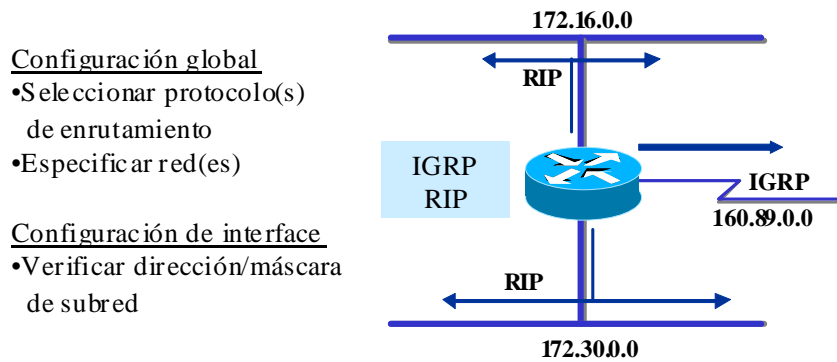
9.16.2 IGRP: Protocolo de enrutamiento por vector de distancia de Cisco.

9.16.3 OSPF: Protocolo de enrutamiento de estado de enlace (link-state).

9.16.4 Enhanced IGRP (EIGRP): Protocolo de enrutamiento híbrido equilibrado.

Tareas de configuración de enrutamiento Dinámico

9.17 Como se indica en la figura, es necesario seleccionar el protocolo de enrutamiento a utilizar desde el modo de configuración global, y a continuación se ingresan tantos subcomandos network como sea necesario para habilitar la actividad del protocolo en las redes correspondientes.

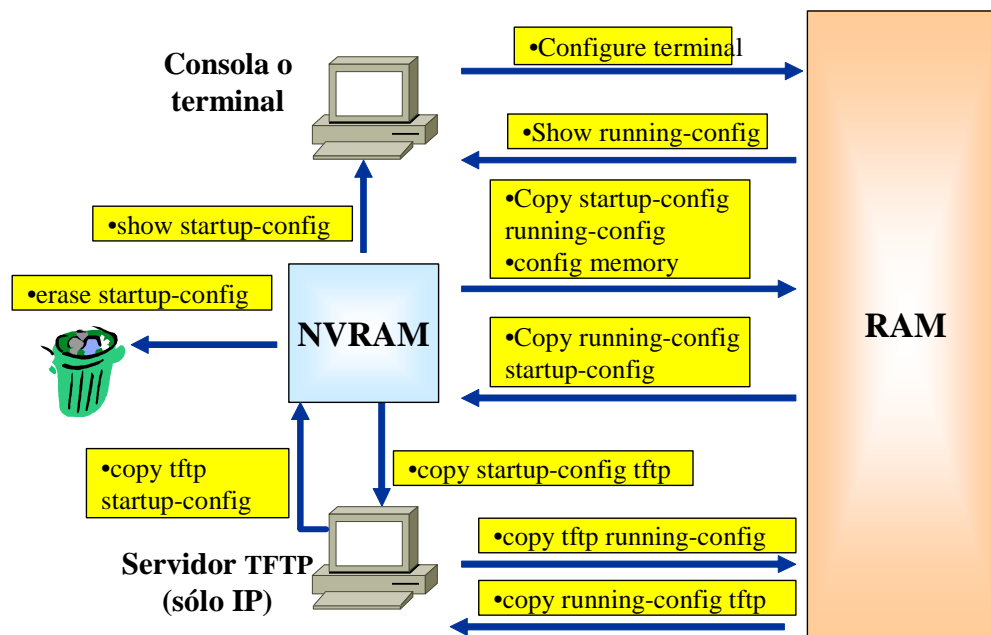


9.18 En la figura se muestra una situación de configuración de un router con 3 interfaces y diferentes protocolos de enrutamiento.

9.19 Debe especificarse mediante el comando global “router” el protocolo de enrutamiento que desea habilitarse.

10. ADMINISTRACIÓN DEL ENTORNO DE CONFIGURACIÓN

10.1 Conforme la red crece y evoluciona, es necesario mantener desde un sitio centralizado el control del software y de los archivos de los dispositivos de la red.



Operaciones con servidor TFTP

10.2 Las configuraciones de los dispositivos pueden almacenarse y descargarse desde un servidor TFTP.

Backup de la configuración

10.3 Se puede almacenar una copia actual de la configuración en un servidor TFTP.

Recuperación de la configuración

10.4 Puede configurar el router recuperando el archivo de configuración almacenado en uno de los servidores de la red.

Convenciones de nombres de Cisco IOS

10.5 Para optimizar la forma en que opera el software en las diversas plataformas, Cisco ha desarrollado muchas imágenes diferentes. Estas imágenes se ajustan a las diversas plataformas, a los recursos de memoria disponibles, y reflejan las necesidades que tienen sus clientes para los dispositivos de la red.

10.6 A lo largo del tiempo, se han acumulado miles de imágenes IOS y conjuntos de características (Feature Sets). Las convenciones sobre la designación de nombres del software Cisco IOS, el significado del nombre del campo, el contenido de la imagen y otros detalles estuvieron siempre sujetos a cambio, debiendo consultarse con frecuencia el sitio Cisco Connection Online (CCO) para obtener datos actualizados.

10.7 A partir de la versión 12.3, Cisco ha simplificado drásticamente la tarea de seleccionar el Feature Set, reduciendo a 8 las alternativas de Feature Sets (de un total de 44 que existían para cada versión previa a la 12.3).

10.8 La siguiente tabla muestra la funcionalidad que se incluye en cada uno de los 8 paquetes de software IOS.

10.9 Como se aprecia, IP BASE es el cimiento sobre el que se construyen los otros 7 paquetes. Así, por ejemplo, si se requiriera voz, deberíamos pensar en paquete IP VOICE.

10.10 Pero, si además fuera necesario incorporar funciones de seguridad (Firewall, IDS y VPN), entonces el paquete adecuado debería ser ENTERPRISE BASE (que incorpora el soporte para ATM, VoATM y MPLS, no requeridos en nuestro caso, pero son las consecuencias de la metodología del packaging decidida por CISCO, en el que ha priorizado la simplicidad).

Funcionalidad	Conectividad Datos	VoIP y VoFR	ATM, VoATM y MPLS	Protocolos AppleTalk, IPX, IBM	Firewall, IDS, VPN
IOS Packaging					
IP Base	X				
IP Voice	X	X			
Advanced Security	X				X
Advanced IP Services	X			X	

SP Services	X	X	X		
Enterprise Base	X	X	X		X
Enterprise Services	X	X	X	X	
Advanced Enterprise Services	X	X	X	X	X

11. ACCESO A OTROS ROUTERS

11.1 Existen diferentes formas de acceder a la información de otros routers. Una de ellas es utilizando el protocolo CDP.

CDP

11.2 El Cisco Discovery Protocol (CDP) ofrece una herramienta, propietaria de Cisco, la cual permite que los administradores de la red accedan a un resumen de la configuración de otros routers directamente conectados. CDP corre sobre la capa de enlace de datos que conecta los medios físicos y los protocolos de las capas superiores. Como CDP opera a bajo nivel, los dispositivos del CDP que soportan diferentes protocolos de la capa de red pueden conocerse entre sí. -la dirección de enlace de datos es similar al concepto de la dirección MAC-.

11.3 Cuando un dispositivo Cisco ejecuta la secuencia inicial, CDP se pone en funcionamiento por omisión, y a partir de allí puede descubrir automáticamente los dispositivos Cisco vecinos que también estén utilizando CDP.

11.4 Los dispositivos descubiertos se extienden más allá de aquellos que tienen TCP/IP, ya que CDP descubre los dispositivos Cisco que estén directamente conectados, independientemente de los protocolos de capa 3 y capa 4 que se encuentren ejecutando.

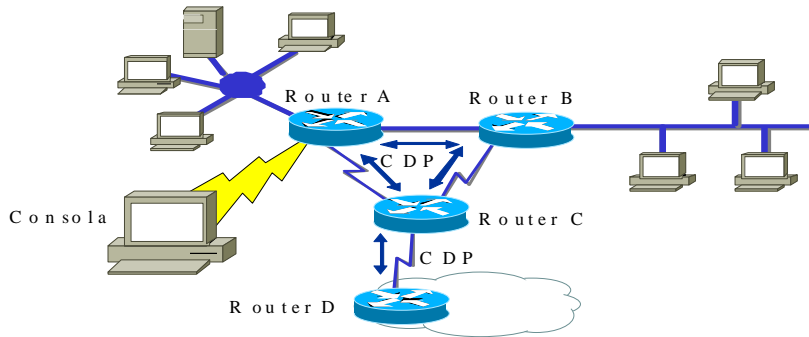
• Direcciones de entrada de la capa superior

• Protocolo de Enlace de Datos propietario de Cisco

• SNAP
Soporte a medios

TCP/IP	AppleTalk
Novell IPX	Otros
El protocolo CDP descubre y muestra información de dispositivos Cisco directamente conectados	
LAN's	ATM
Frame Relay	Otros

Información CDP



11.5 En el gráfico se ve un ejemplo de la forma en la que CDP ofrece sus beneficios al administrador del sistema.

11.6 Cada router que ejecuta CDP intercambia información relacionada con los datos de cualquier protocolo que conozca con sus vecinos.

11.7 El administrador puede ver en pantalla los resultados de este intercambio de información del CDP en una consola conectada a un router configurado para ejecutar el CDP en sus interfaces.

11.8 El administrador de red utiliza un comando **show** para visualizar en pantalla la información sobre las redes directamente conectadas al router. CDP brinda información sobre cada dispositivo vecino CDP. Entre los posibles datos se incluyen:

11.8.1 **Identificadores de dispositivos:** Por ejemplo, el nombre del host y el nombre de dominio (si lo hubiera) configurados en el router.

11.8.2 **Lista de direcciones:** Una dirección por cada protocolo que esté soportando.

11.8.3 **Identificador de puertos:** Por ejemplo Ethernet 0, Ethernet 1, Serial 0, etc.

11.8.4 **Lista de capacidades:** Por ejemplo si el dispositivo actúa como bridge de ruta de origen además de como router.

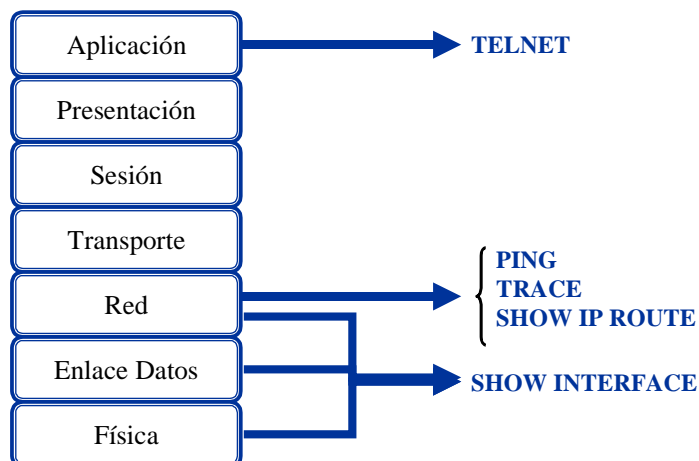
11.8.5 **Versión:** Información como la que ofrece el comando show versión, ejecutado localmente.

11.8.6 **Plataforma:** Plataforma del hardware del dispositivo: por ejemplo, Cisco 7000.

11.9 El router ubicado más abajo en la figura no está directamente conectado al router de la consola del administrador. Por consiguiente, para obtener información de CDP sobre este dispositivo, el administrador necesitaría efectuar una conexión por Telnet con un router directamente conectado a este objetivo.

Proceso de Testing

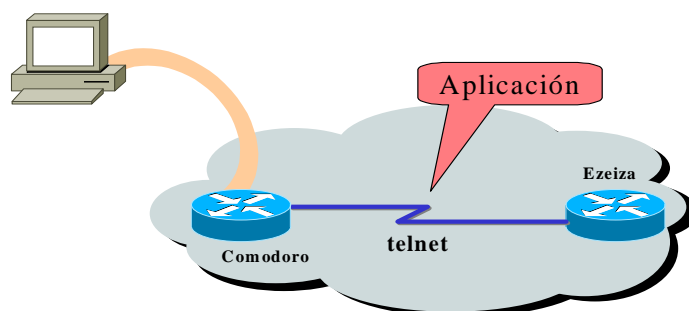
11.10 La prueba básica de una red debería provenir en secuencia desde una capa del modelo ISO/OSI hacia la siguiente. Cada prueba que se presenta en esta sección se refiere a las operaciones de red de una capa específica del modelo OSI.



Testing de la Capa de Aplicación

11.11 Telnet ofrece un servicio de terminal virtual, de modo que el administrador pueda utilizar las operaciones Telnet para conectarse con otros hosts que utilicen TCP/IP (a través de la conexión de una aplicación cliente a una aplicación servidor)

11.12 La prueba tiene el objetivo de determinar si es posible acceder al router remoto. Por ejemplo, ejecutar con éxito Telnet para conectarse desde el router Comodoro con el otro router Ezeiza es una prueba básica para comprobar la conectividad y accesibilidad.



11.13 Si podemos acceder remotamente a otro router a través de Telnet, no solamente se comprobará que una aplicación TCP/IP –aplicación de capa superior- puede llegar al router remoto, sino que también indicará que los servicios de las capas inferiores también funcionan correctamente.

11.14 Si es posible la comunicación vía Telnet con un router pero no con otro router, es probable que el fallo de Telnet esté causado por un nombre de dirección específico o con problemas de permiso de acceso. Estos problemas pueden estar en nuestro router o en el router que falló como objetivo de la comunicación Telnet.

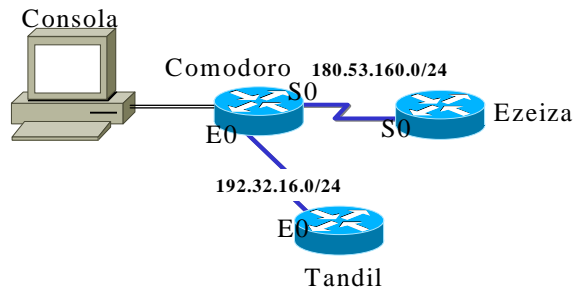
Testing de la Capa de Red

11.15 Las siguientes herramientas permiten dictaminar la salud de la capa de red.

Comando Ping

11.16 Como ayuda para diagnosticar la conectividad básica de la red, muchos protocolos de red soportan un protocolo de eco, que es una prueba para determinar si se están enrutando correctamente los paquetes del protocolo.

```
COMODORO>ping 180.53.160.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.53.160.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
COMODORO>
```



11.17 El comando **ping** envía un paquete especial al host de destino y luego espera un paquete de respuesta de dicho host. Los resultados de este protocolo de eco pueden ayudar a evaluar la confiabilidad de la ruta al host, las demoras de la ruta y si se puede llegar al host y si éste está funcionando.

11.18 En el gráfico, el objetivo **ping 180.53.160.2** respondió exitosamente a cuatro de los cinco datagramas que se le enviaron. Los signos de exclamación (!) indican cada eco exitoso. Si en vez de recibir estos signos se recibieran uno o más puntos (.), significa que la aplicación del router local se dio por vencido (time out) esperando el eco de un paquete.

11.19 El comando de usuario EXEC **ping** puede utilizarse para diagnosticar la conectividad básica de la red. El protocolo que utiliza ping es ICMP (Internet Control Message Protocol).

Comando trace

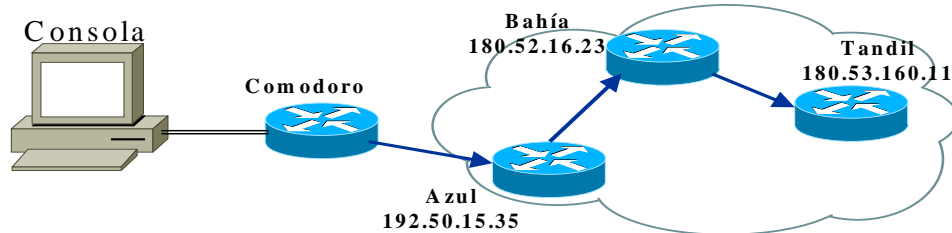
11.20 El comando trace es la herramienta ideal para descubrir a dónde se están enviando los datos en su red. Utiliza el mismo protocolo que el ping, salvo que en lugar de probar la conectividad de extremo a extremo, el comando trace prueba cada paso del camino.

11.21 Esta operación puede realizarse desde cualquiera de los niveles EXEC: usuario o privilegiado.

11.22 El comando trace aprovecha los mensajes de error generados por los routers cuando un paquete excede su valor de tiempo de existencia (TTL), envía varios paquetes y exhibe en pantalla el tiempo de ida y vuelta de cada uno.

11.23 El beneficio del comando trace es que nos dice cuál es el último router de la ruta al que se llega. Esto se denomina aislamiento de fallos.

11.24 En el ejemplo, se rastrea la ruta desde Comodoro hacia Tandil. En su camino, la ruta debe ir a través de Azul y Bahía. Si uno de estos routers no se hubiera podido alcanzar, habríamos visto tres asteriscos (*) en lugar del nombre del router. El comando trace continuaría intentando llegar al próximo paso hasta que hiciéramos una operación de escape.



```
comodoro>trace azul

Type escape sequence to abort.
Tracing the route to azul (180.53.160.11)

 0  azul (192.50.15.35)  4 msec  8 msec  12 msec
 1  bahia (180.52.16.23) 6 msec 10 msec 14 msec
 2  tandil (180.53.160.11) 8 msec 14 msec 16 msec

COMODORO>
```

Comando show ip route

11.25 El router nos brinda algunas herramientas poderosas en este punto de nuestra búsqueda. Podemos efectivamente ver la tabla de enrutamiento – es decir las direcciones que utiliza el router para determinar cómo direccionar el tráfico por la red-.

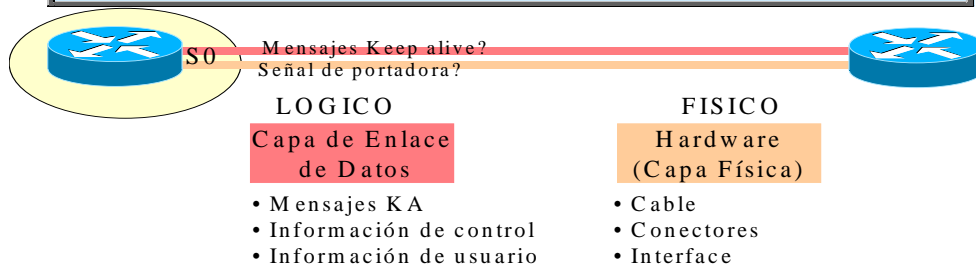
Operatividad del enlace

11.26 El hardware debe efectuar la conexión real entre los dispositivos. El software son los mensajes que se intercambian entre los dispositivos adyacentes. Esta información está constituida por datos que se pasan entre dos interfaces del router conectadas.

La interface tiene dos componentes:

- > Físico (hardware)
- > Lógico (software).

```
COMODORO>show interface serial 0
Serial0 is up, line protocol is up
Hardware is HD64570
Description: INTERFACE SERIE HACIA EZEIZA
Internet address is 192.168.12.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```



11.27 Cuando se comprueba el enlace físico y el enlace de datos, se formulan estas preguntas:

11.27.1 ¿Hay una señal de detección de portadora?

11.27.2 ¿Está operativo el enlace físico entre los dispositivos?

11.27.3 ¿Se están recibiendo los mensajes de actividad (KA)?

11.27.4 ¿Se pueden enviar paquetes de datos a través del enlace físico?

Comando show interface serial

11.28 Uno de los elementos más importantes del resultado del comando **show interface serial** es la representación en pantalla del estado de la línea y el del protocolo de enlace de datos. El gráfico indica la línea de resumen clave que se debe verificar y los significados del estado.

INTERPRETACIÓN DE LA INFORMACIÓN: show interface serial		
FÍSICO	LÓGICO	ESTADO
UP	UP	Operacional
UP	DOWN	Problema de conexión
DOWN	DOWN	Problema de interface
DOWN Administrativo	DOWN	Deshabilitada

11.29 El estado de la línea, en este ejemplo, está condicionado por la señal de detección de portadora y se refiere al estado de la capa física.

11.30 Sin embargo, el protocolo de línea, está condicionado por los frames de actividad, es decir que se aplica a las tramas del enlace de datos.

Tráfico en tiempo real

11.31 El router incluye hardware y software que permiten rastrear problemas del mismo router o de otros hosts de la red. El comando EXEC **debug** del nivel privilegiado da inicio a la representación en la consola de los hechos ocurridos en la red, que se hayan indicado en el parámetro del comando debug.

FUNCIONES DE ENRUTAMIENTO

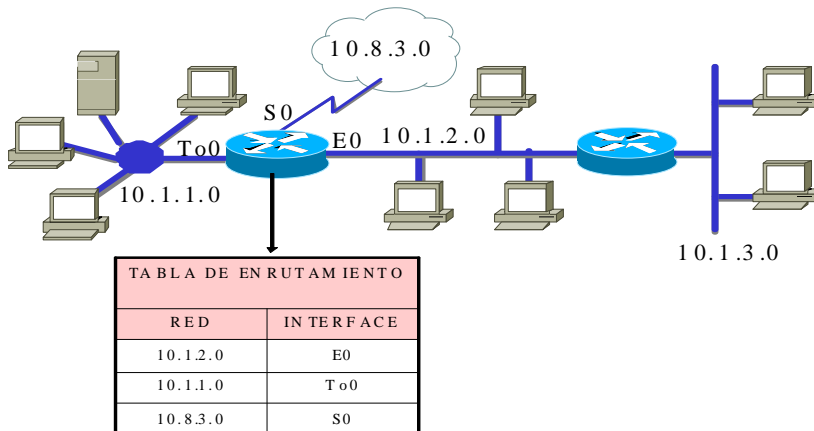
CLASES DE PROTOCOLOS DE ENRUTAMIENTO

1. FUNCIONES DE ENRUTAMIENTO

1.1 Es posible configurar a los routers para que utilicen uno o más protocolos de enrutamiento IP (o de otro protocolo de red). No existe un único algoritmo de enrutamiento que satisfaga los requerimientos de cualquier red. Los administradores de las redes deben analizar diferentes aspectos (técnicos y políticos) para escoger el mejor algoritmo.

CONSIDERACIONES DE ENRUTAMIENTO

Tabla inicial de enrutamiento IP



1.2 Inicialmente, un router debe referirse a las entradas de las redes y subredes que se conectan directamente. Cada interface debe ser configurada con una máscara y una dirección IP. El software IOS de Cisco debe recibir la dirección IP y máscara como información de entrada de configuración de alguna fuente. La fuente inicial de direccionamiento es de la persona que realiza la primera configuración.

1.3 Los routers, por defecto conocen las rutas a destinos de tres modos distintos:

1.3.1 Rutas estáticas -Definidas manualmente por el administrador del sistema como la única ruta hacia el destino. Son útiles para controlar la seguridad y reducir el tráfico.

1.3.2 Rutas por defecto - Definidas manualmente por el administrador del sistema como la ruta a tomar cuando no existe una ruta conocida hacia el destino.

1.3.3 Enrutamiento dinámico - El router se entera de las rutas a los destinos al recibir actualizaciones periódicas de otros routers.

Configuración de ruta estática

1.4 El siguiente comando establece una ruta estática:

Comando ip route	Descripción
network	Red o subred de destino
mask	Máscara de subred
address	Dirección IP del router del próximo salto
interface	Nombre de la interface que se utilizará en la red de destino
distance	Distancia administrativa

1.5 La distancia administrativa es una clasificación de confiabilidad de una fuente de información de enrutamiento, expresada como un valor numérico de 0 a 255. Cuanto mayor es el valor, menos es la clasificación de confiabilidad.

1.6 Una ruta estática permite una configuración manual de la tabla de enrutamiento. No se producirán cambios dinámicos en una entrada de tabla determinada mientras esté activa la ruta.

1.7 Una ruta estática puede reflejar algún conocimiento especial de la situación de networking conocida para el administrador de red. Los valores de distancia administrativa ingresados manualmente son en general números bajos.

1.8 Las actualizaciones de enrutamiento no se envían por un enlace, si sólo son definidas por una ruta estática, y de este modo se conserva el ancho de banda.

Ejemplo:

Comando: ip route 172.16.1.0 255.255.255.0 172.16.2.1	
Comando	Descripción
ip route 172.16.1.0	Especifica una ruta estática a la subred de destino.
255.255.255.0	Una máscara de subred indica que hay 8 bits de conexión en subredes en curso.
172.16.2.1	Dirección IP del router del próximo salto en la ruta al destino.

Configuración de ruta por defecto

Comando ip default network	Descripción
network-number	Número de red IP o número de subred definido como defecto.

1.9 Cuando no existe una entrada para la red de destino en la tabla de enrutamiento, el paquete se envía a la red por defecto. La red por defecto debe existir en la tabla de enrutamiento. Las rutas por defecto mantienen la longitud de las tablas de enrutamiento más cortas.

1.10 Debe utilizarse una red por defecto cuando solamente se posea información parcial sobre la red de destino. Como el router no tiene un conocimiento completo de todas las redes de destino, puede usar un número de red por defecto para indicar la dirección a tomar para números de redes desconocidos.

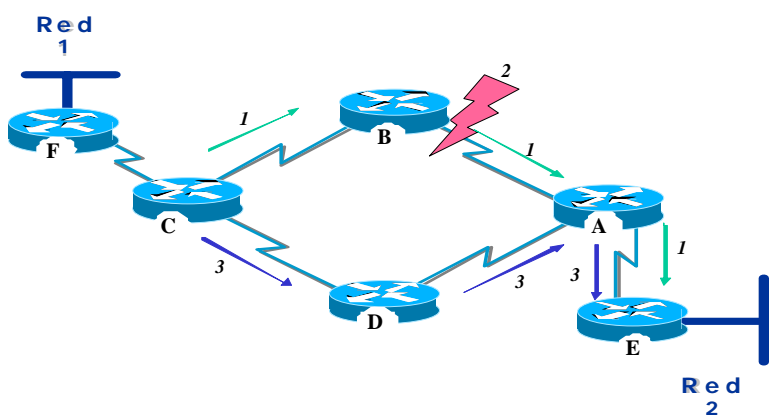
1.11 Por ejemplo el comando global `ip default-network 192.168.17.0` define la red de clase C 192.168.17.0, como la ruta de destino para los paquetes que no tienen una entrada en una tabla de enrutamiento.

Rutas estáticas versus rutas dinámicas

1.12 El conocimiento estático se administra en forma manual: un administrador de red la ingresa en la configuración del router. El administrador debe actualizar manualmente esta entrada de ruta estática¹⁵ cada vez que un cambio de topología de internetwork requiera una actualización.

1.13 El conocimiento dinámico funciona de modo diferente. Después de que el administrador de red ingresó los comandos de configuración para iniciar el enrutamiento dinámico¹⁶, el conocimiento de la ruta se actualiza automáticamente por un proceso de enrutamiento cada vez que se recibe nueva información de la internetwork. Los cambios en el conocimiento dinámico se intercambian entre routers como parte del proceso de actualización.

Adaptación al cambio de topología



1.14 La red que se muestra en el gráfico se adapta de distintas formas al cambio de topología según utilice conocimiento configurado estática o dinámicamente. El enrutamiento estático permite a los routers enrutar un paquete en forma adecuada de una red a otra. El router se remite a su tabla de enrutamiento y sigue el conocimiento estático hasta allí para pasar el paquete al router F, C, B, A y E, hasta entregar el paquete al host de destino.

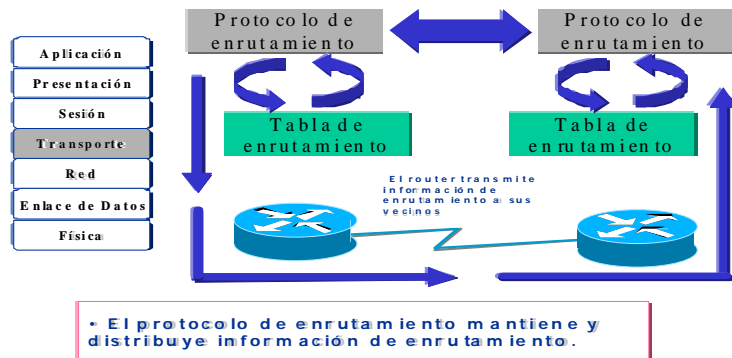
1.15 Pero, ¿qué sucede si falla la ruta entre el router B y el router A? Obviamente, el router B no podrá transmitir el paquete al router A con una ruta estática. Hasta que el router C no sea reconfigurado manualmente para pasar los paquetes por medio del router D, la comunicación con la red de destino es imposible.

¹⁵ **Ruta estática** - Ruta explícitamente configurada e ingresada en la tabla de enrutamiento. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico.

¹⁶ **Enrutamiento dinámico** - Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico. También denominado *enrutamiento adaptable*.

1.16 El enrutamiento dinámico ofrece flexibilidad. Según la tabla de enrutamiento generada por el router C, un paquete puede llegar a su destino por la ruta preferida a través del router B. Sin embargo, existe una ruta alternativa disponible a través del router D. Cuando el router B reconoce que el enlace al router A está caído, ajusta su tabla de enrutamiento, y pasa la información al router C, quién selecciona la ruta a través del router D como ruta preferida hacia su destino. Los routers continúan enviando paquetes a través de este enlace.

1.17 Cuando la ruta entre los routers B y A reanuda su servicio, el router C puede cambiar nuevamente su tabla de enrutamiento e indicar su preferencia por la ruta en el sentido de las agujas del reloj a través de los routers B y A hacia la red de destino. Los protocolos de enrutamiento dinámico también pueden redirigir el tráfico entre las diferentes rutas de una red.



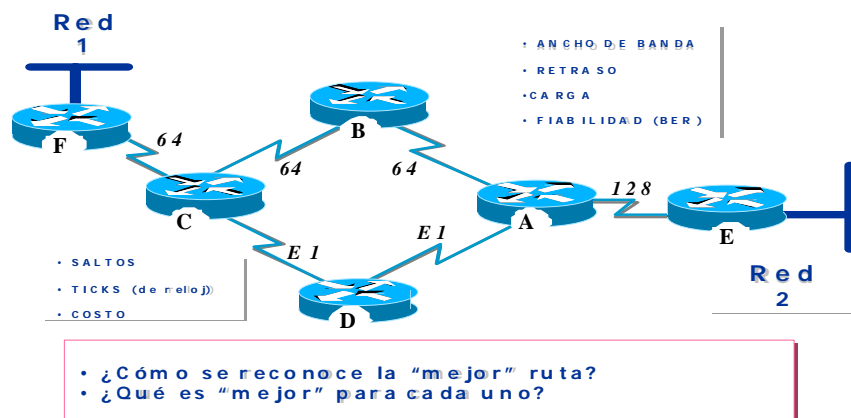
ENRUTAMIENTO DINÁMICO

1.18 El éxito del enrutamiento dinámico depende de dos funciones básicas del router:

1.18.1 Mantenimiento de una tabla de enrutamiento

1.18.2 Distribución a tiempo del conocimiento — en forma de actualizaciones de enrutamiento — a otros routers.

1.19 El enrutamiento dinámico se basa en un protocolo de enrutamiento para compartir el conocimiento. Un protocolo de enrutamiento define el conjunto de reglas utilizadas por el router para comunicarse con sus vecinos.



1.20 Por ejemplo, un protocolo de enrutamiento describe:

1.20.1 Cómo se envían las actualizaciones

1.20.2 Qué información contienen dichas actualizaciones

- 1.20.3 Cuándo enviar esta información
- 1.20.4 Cómo localizar los receptores de las actualizaciones

Representación de distancias mediante métricas

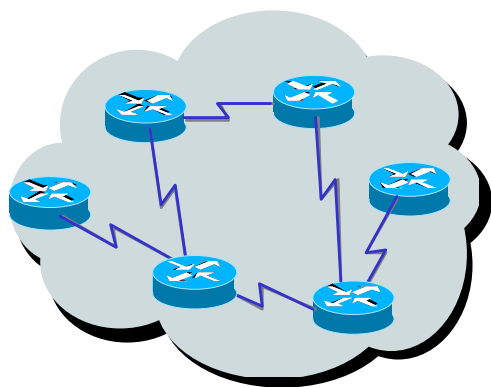
1.21 Cuando un algoritmo de enrutamiento actualiza una tabla de enrutamiento, su objetivo principal es determinar la mejor información para incluirla en la tabla. Cada algoritmo de enrutamiento interpreta el término: mejor, a su propio modo. El algoritmo genera un número -denominado valor de métrica- para cada ruta a través de la red. Cuanto menor sea el número de métrica, mejor será la ruta.

1.22 Las métricas se pueden calcular basándose en una sola característica de la ruta. Se pueden calcular métricas más complejas combinando varias características. Se utilizan varias características de ruta en el cálculo de las métricas. Las métricas que los routers utilizan más comúnmente son las siguientes:

- 1.22.1 **Ancho de banda** - Capacidad de datos de un enlace. Por ejemplo, normalmente, un enlace Ethernet de 10 Mbps es preferible a una línea arrendada de 64 kbps.
- 1.22.2 **Retraso** - Tiempo necesario para mover un paquete desde el origen hasta el destino.
- 1.22.3 **Carga** - Cantidad de actividad en un recurso de red, como un router o un enlace.
- 1.22.4 **Fiabilidad** - Generalmente se refiere a la tasa de error de cada enlace de red.
- 1.22.5 **Número de saltos** - Cantidad de routers que debe atravesar un paquete.
- 1.22.6 **Ticks** - Retraso en un enlace de datos utilizando ticks del reloj de una PC IBM (aproximadamente 55 milisegundos).
- 1.22.7 **Costo** - Valor arbitrario, en general basado en el ancho de banda, gasto en pesos, dólares u otra medida, que lo asigna el administrador de red

Sistema autónomo

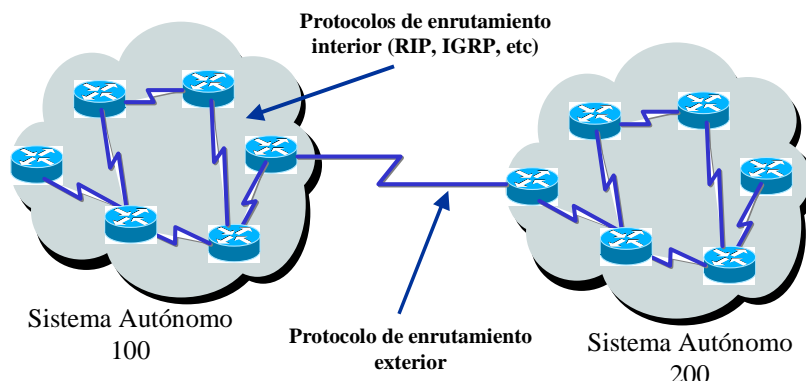
1.23 Un sistema autónomo consiste en routers, administrados por uno o más operadores, que presentan una pauta coherente de enrutamiento hacia el mundo externo.



1.24 El Centro de información de la red [Network Information Center] (NIC) asigna un sistema autónomo exclusivo a las empresas. Este sistema autónomo es un número de 16 bits. Un protocolo de enrutamiento como el Protocolo de enrutamiento de gateway interior de Cisco [*Interior Gateway Routing Protocol*] (IGRP) demanda que especifique este número de sistema autónomo exclusivo asignado en su configuración.

PROTOCOLOS INTERIORES Y EXTERIORES

1.25 Se utilizan protocolos de enrutamiento exteriores para comunicar entre sistemas autónomos. Se utilizan protocolos de enrutamiento interiores dentro de un único sistema autónomo.



Protocolos de enrutamiento IP interiores

1.26 En la capa de Internet del conjunto de protocolos TCP/IP, un router puede usar protocolos de enrutamiento a través de algoritmos específicos. Los ejemplos de protocolos de enrutamiento IP incluyen:

- 1.26.1 RIP—Un protocolo de enrutamiento por vector de distancia.
- 1.26.2 IGRP— Un protocolo de enrutamiento por vector de distancia de Cisco.
- 1.26.3 OSPF—Un protocolo de enrutamiento de estado de enlace.
- 1.26.4 EIGRP (Enhanced IGRP) —Un protocolo de enrutamiento híbrido equilibrado.

2. CLASES DE PROTOCOLOS DE ENRUTAMIENTO

2.1 La mayoría de los algoritmos de enrutamiento se pueden clasificar en uno de dos tipos de algoritmos básicos: vector de distancia¹⁷ o estado de enlace¹⁸.

2.2 El tipo de enrutamiento por vector de distancia determina la dirección (vector) y la distancia a cualquier enlace en la internetwork.

2.3 El tipo de enrutamiento de estado de enlace (también llamado de la ruta más corta - SPF) recrea la topología exacta de toda la internetwork (o al menos la partición donde está situado el router).

¹⁷ **Algoritmo de enrutamiento por vector de distancia (Bellman-Ford)** - Clase de algoritmos de enrutamiento que iteran sobre el número de saltos en una ruta para encontrar un spanning-tree de camino más corto. Los algoritmos de enrutamiento por vector de distancia envían a sus vecinos su tabla de enrutamiento total en cada actualización. Los algoritmos de enrutamiento por vector de distancia son propensos a los bucles de enrutamiento, pero son computacionalmente más simples que los algoritmos de enrutamiento del estado de enlace.

¹⁸ **Algoritmo de enrutamiento del estado de enlace** - Algoritmo de enrutamiento en el cual cada router realiza un broadcast o multicast de información a todos los nodos de la internetwork con el costo de comunicación hacia cada uno de sus vecinos. Los algoritmos de estado de enlace crean una vista consistente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero al costo de dificultades computacionales relativamente mayores y un tráfico más diseminado (comparado con los algoritmos de enrutamiento por vector de distancia).

2.4 El tipo de híbrido balanceado combina aspectos de los algoritmos de estado de enlace y por vector de distancia.

Convergencia

2.5 El algoritmo de enrutamiento es esencial para el enrutamiento dinámico. Cuando la topología de la red cambia debido a crecimiento, reconfiguración, o fallas, el conocimiento base de la red también debe cambiar.

2.6 El conocimiento necesita reflejar una visión precisa y consistente de la nueva topología. Esta visión precisa y consistente se denomina convergencia.

2.7 Cuando todos los routers de una internetwork trabajan con la misma información, se dice que la internetwork ha convergido.

2.7.1 La convergencia tiene lugar cuando todos los routers utilizan una perspectiva consistente de la topología de la red. 2.7.2 Cada vez que la topología cambia, los routers deben recalculan las rutas, provocando un estado de transición.

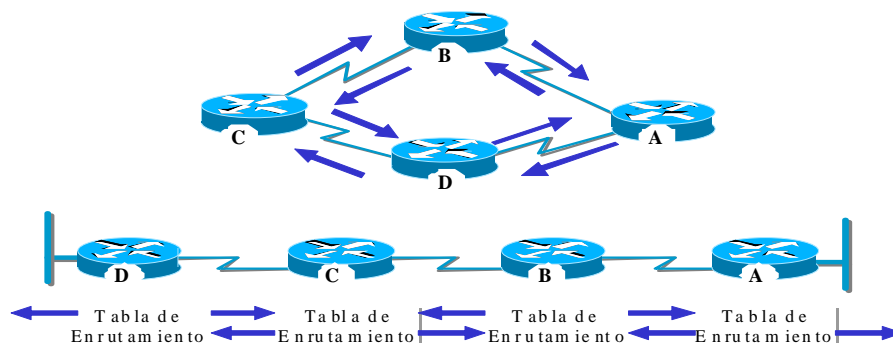
2.7.3 El proceso y el tiempo requeridos para la convergencia varían con los protocolos de enrutamiento. 2.8 La convergencia rápida es una característica de red conveniente, porque reduce el período en que los routers tienen conocimiento desactualizado, para así evitar tomar decisiones de enrutamiento que podrían ser incorrectas, antieconómicas, o ambas cosas a la vez.

VECTOR DISTANCIA

2.9 Los algoritmos de enrutamiento por vector de distancia (también conocidos como algoritmos Bellman-Ford) transmiten copias periódicas de una tabla de enrutamiento de un router a otro. Las actualizaciones regulares entre routers comunican los cambios de topología.

2.10 Cada router recibe una tabla de enrutamiento de su vecino directo. Por ejemplo, en la figura siguiente, el router B recibe información del router A.

2.11 El router B agrega un número de vector de distancia (tal como una cantidad de saltos) que aumenta el vector de distancia, y luego transmite la tabla de enrutamiento a su otro vecino, el router C. Este mismo proceso paso a paso ocurre en todas las direcciones entre routers vecinos directos.

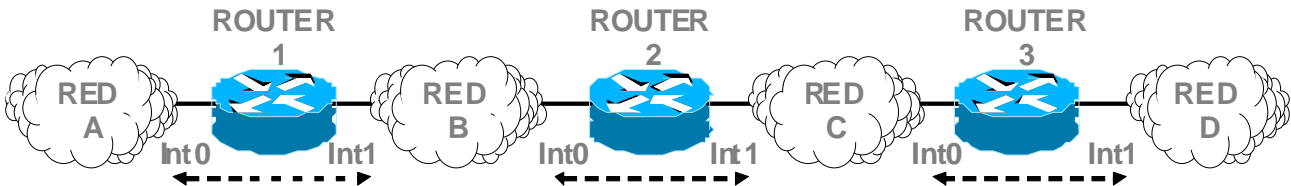


2.12 De este modo, el algoritmo acumula distancias de red para poder mantener una base de datos de información de topología de la red.

2.13 Los algoritmos de vector de distancia no permiten al router conocer la topología exacta de una internetwork.

Descubrimiento de la red por vector de distancia

2.14 Cada router que utiliza el enrutamiento por vector de distancia comienza identificando sus propias redes (conectadas directamente). En el gráfico, el puerto hacia cada red conectada directamente tiene una distancia de 0.



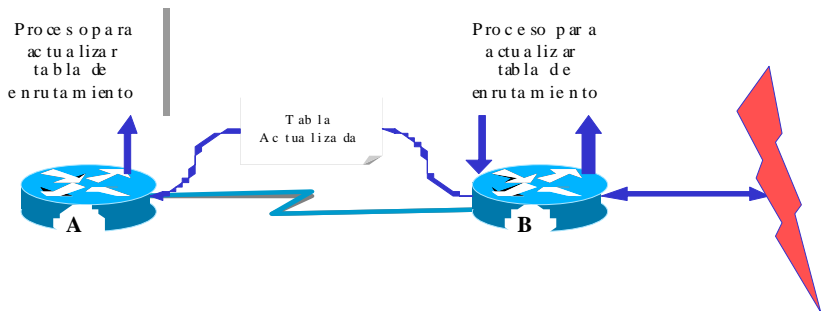
A medida que el proceso de descubrimiento de la red por vector de distancia sigue su curso, los routers descubren la mejor ruta hacia las redes de destino basándose en información de cada vecino.

ROUTER 1	ROUTER 2	ROUTER 3
A → Int0 → 0 B → Int1 → 0	B → Int0 → 0 C → Int1 → 0	C → Int0 → 0 D → Int1 → 0
A → Int0 → 0 B → Int1 → 0 C → Int1 → 1	B → Int0 → 0 C → Int1 → 0 A → Int0 → 1 D → Int1 → 1	C → Int0 → 0 D → Int1 → 0 B → Int0 → 1
A → Int0 → 0 B → Int1 → 0 C → Int1 → 1 D → Int1 → 2	B → Int0 → 0 C → Int1 → 0 A → Int0 → 1 D → Int1 → 1	C → Int0 → 0 D → Int1 → 0 B → Int0 → 1 A → Int0 → 2

2.15 Por ejemplo, el router A adquiere conocimientos acerca de otras redes basándose en información que recibe del router B. Cada una de estas entradas de otras redes en la tabla de enrutamiento tiene un vector de distancia acumulado para mostrar a qué distancia está la red en la dirección dada.

Cambios en la topología por vector de distancia

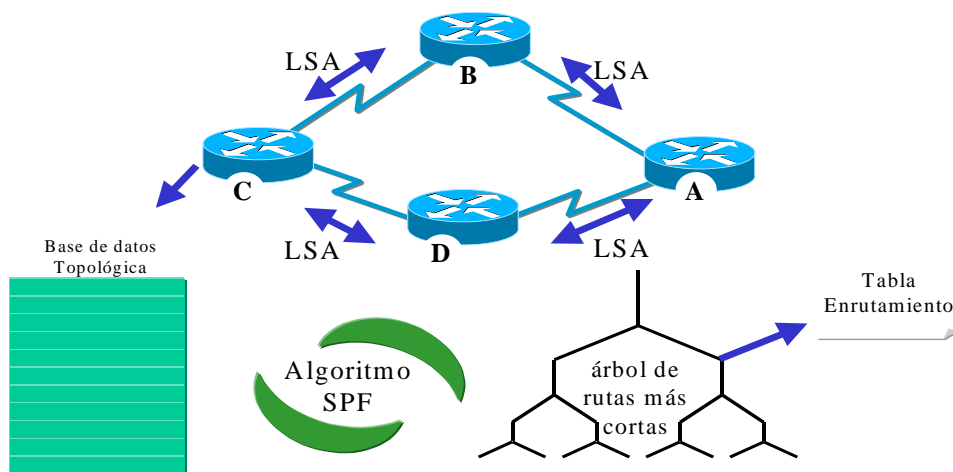
2.16 Cuando cambia la topología en un protocolo por vector de distancia, deben efectuarse actualizaciones de la tabla de enrutamiento. Al igual que en el proceso de descubrimiento de la red, las actualizaciones de cambio de topología tienen lugar paso a paso de router a router.



2.17 Los algoritmos por vector de distancia requieren a cada router que envíe toda su tabla de enrutamiento a cada uno de sus vecinos adyacentes. Las tablas de enrutamiento por vector de distancia incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada red que conoce.

ESTADO DE ENLACE

2.18 Los algoritmos de enrutamiento basados en el estado de enlace - también conocidos como algoritmos de la ruta más corta (SPF) - mantienen una base de datos compleja de información de la topología. Mientras que el algoritmo por vector de distancia tiene información inespecífica acerca de redes distantes y no tiene conocimiento acerca de routers distantes, un algoritmo del estado de enlace mantiene el conocimiento completo de los routers distantes y de cómo se interconectan.



2.19 El enrutamiento del estado de enlace utiliza las publicaciones del estado de enlace (LSAs)¹⁹, una base de datos topológica, el algoritmo SPF²⁰, el árbol SPF resultante, y finalmente, una tabla de enrutamiento de rutas y puertos hacia cada red. Las siguientes páginas explican estos procesos y bases de datos más detalladamente.

2.20 Los ingenieros han implementado este concepto de estado de enlace en el enrutamiento primero la ruta libre más corta (OSPF). RFC 1583 contiene una descripción de los conceptos y operaciones del estado de enlace OSPF.

Descubrimiento de la red por estado de enlace

2.21 El descubrimiento de la red para el enrutamiento por estado de enlace utiliza los siguientes procesos:

¹⁹ **LSA** - (Link-state advertisement) ó *Paquete del estado de enlace (LSP)*. Publicación del estado de enlace. Paquete de broadcast utilizado por los protocolos por estado de enlace que contiene información acerca de los vecinos y los costos de ruta. Los LSAs son utilizados por los routers receptores para mantener sus tablas de enrutamiento.

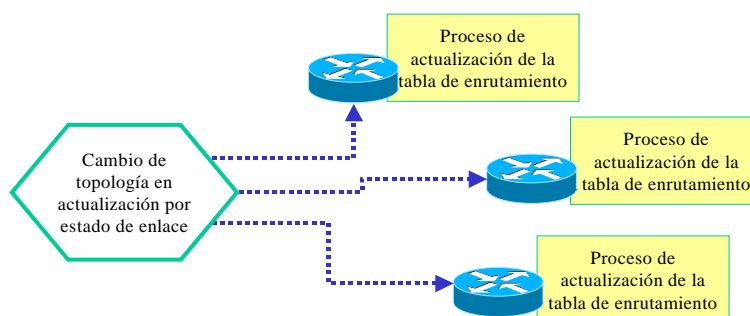
²⁰ **SPF** - (shortest path first algorithm) Algoritmo de enrutamiento que itera sobre la longitud de la ruta para determinar el spanning tree de la ruta más corta. *Algoritmo de Dijkstra*.

2.21.1 Los routers intercambian las LSA entre sí. Cada router comienza con las redes directamente conectadas sobre las cuales tiene información directa. A continuación, cada router en paralelo con los otros, construye una base de datos topológica que incluye todas las LSA de la internetwork.

2.21.2 El algoritmo SPF computa la forma en que se puede llegar a la red, determinando la ruta más corta a cada una de las otras redes de la internetwork de protocolo del estado de enlace. El router construye esta topología lógica de rutas más cortas como un árbol SPF. Consigo mismo como raíz, este árbol expresa rutas desde el router hacia todos los destinos. El router hace una lista con sus mejores rutas y con los puertos hacia dichas redes de destino en la tabla de enrutamiento. También lleva otras bases de datos de elementos topológicos y detalles sobre el estado

Cambios en la topología por estado de enlace

2.22 Los algoritmos del estado de enlace se basan en el uso de las mismas actualizaciones del estado de enlace. Cada vez que se modifica una topología del estado de enlace, los routers que primero conocen dichas modificaciones envían información a los otros routers o a un router designado que todos los demás puedan utilizar para sus actualizaciones. Esto incluye el envío de información común de enrutamiento a todos los routers de la internetwork. Para lograr la convergencia, cada router hace lo siguiente:



2.22.1 Lleva un registro de sus vecinos: nombre del vecino, si el vecino está activo o caído, y costo del enlace hacia el vecino. Construye un paquete LSA que contiene una lista de los nombres y costos de enlace hacia sus routers vecinos. Esto incluye nuevos vecinos, modificaciones en el costo del enlace y enlaces hacia vecinos fuera de servicio.

2.22.2 Envía este paquete de LSA de modo que reciban todos los otros routers. Cuando recibe un paquete de LSA, registra el paquete de LSA en su base de datos de modo de poder almacenar el paquete más recientemente generado de todos los demás routers.

2.22.3 Utilizando los datos de los paquetes de LSA acumulados para construir un mapa completo de la topología de la internetwork, procede desde este punto de inicio común a volver a correr el algoritmo SPF y a computar las rutas hacia cada destino de la red.

2.22.4 Cada vez que un paquete de LSA da origen a una modificación en la base de datos del estado de enlace, el algoritmo del estado de enlace vuelve a calcular las mejores rutas y actualiza la tabla de enrutamiento. Luego todos los otros routers toman en cuenta la modificación de la topología para determinar la ruta más corta que pueden utilizar para la conmutación de paquetes.

COMPARACIÓN VECTOR DISTANCIA - ESTADO DE ENLACE

2.23 El enrutamiento por vector de distancia puede compararse con el enrutamiento del estado de enlace en varias áreas clave:

2.23.1 El enrutamiento por vector de distancia obtiene todos los datos topológicos de la información de la tabla de enrutamiento de sus vecinos. El enrutamiento del estado de enlace obtiene una visión amplia de toda la topología de la red acumulando todas las LSA necesarios.

2.23.2 El enrutamiento por vector de distancia determina la mejor ruta aumentando el valor de la métrica que recibe a medida que las tablas pasan de un router a otro. Para el enrutamiento del estado de enlace, cada router trabaja en forma separada para calcular su propia ruta más corta hacia los destinos.

2.23.3 En la mayoría de los protocolos de enrutamiento por vector de distancia, las actualizaciones de cambios de topología tienen lugar como actualizaciones periódicas de las tablas. Estas tablas se transmiten de un router a otro, lo que generalmente da como resultado una convergencia más lenta.

2.23.4 En los protocolos de enrutamiento del estado de enlace, las actualizaciones son causadas generalmente por cambios de topología. Las relativamente pequeñas LSA que son transmitidas a todos los otros routers suelen dar como resultado un tiempo más rápido para la convergencia en cualquier cambio de topología de la red.

VECTOR DISTANCIA	ESTADO DEL ENLACE
<p>Ve la topología de la red desde la perspectiva de los vecinos.</p> <p>Agrega Vectores distancia de router a router.</p> <p>Actualizaciones frecuentes periódicas: convergencia lenta.</p> <p>Pasa copias de la tabla de enrutamiento a los vecinos.</p>	<p>Obtiene una vista común de toda la topología de la red.</p> <p>Calcula la ruta más corta a los otros routers.</p> <p>Actualizaciones disparadas por eventos: convergencia más rápida.</p> <p>Pasa actualizaciones de enrutamiento por estado del enlace a otros routers.</p>

3. CONFIGURACIÓN DE ENRUTAMIENTO DINÁMICO

3.1 La selección de IP como protocolo de enrutamiento implica determinar parámetros tanto globales como de interface.

3.2 Tareas globales:

3.2.1 Seleccionar un protocolo de enrutamiento, RIP o IGRP.

3.2.2 Asignar números de red IP sin especificar valores de subred.

3.3 La tarea de interface es asignar direcciones de red/subred así como la máscara de red correcta. Un enrutamiento dinámico utiliza broadcasts y multicasts para comunicarse con otros routers. La métrica de enrutamiento ayuda a los routers a encontrar la mejor ruta a cada red o subred.

4. RIP

4.1 El protocolo RIP se especificó originalmente en RFC 1058. Las características claves de RIP incluyen las siguientes:

4.1.1 Es un protocolo de enrutamiento por vector de distancia.

4.1.2 Utiliza un cálculo de saltos como métrica para la selección de la ruta.

4.1.3 El cálculo de saltos máximo permisible es 15 (16 es inaccesible).

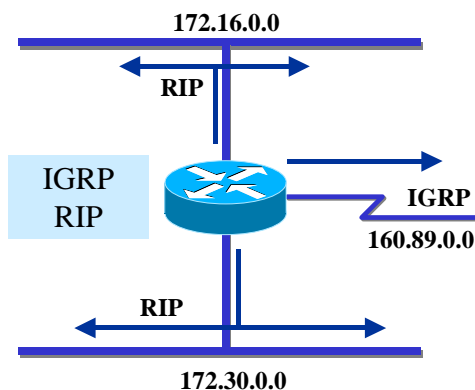
- 4.1.4 Las actualizaciones de enrutamiento se emiten cada 30 segundos por defecto.

Configuración global

- Seleccionar protocolo(s) de enrutamiento
- Especificar red(es)

Configuración de interface

- Verificar dirección/máscara de subred



Ejemplo de configuración de RIP

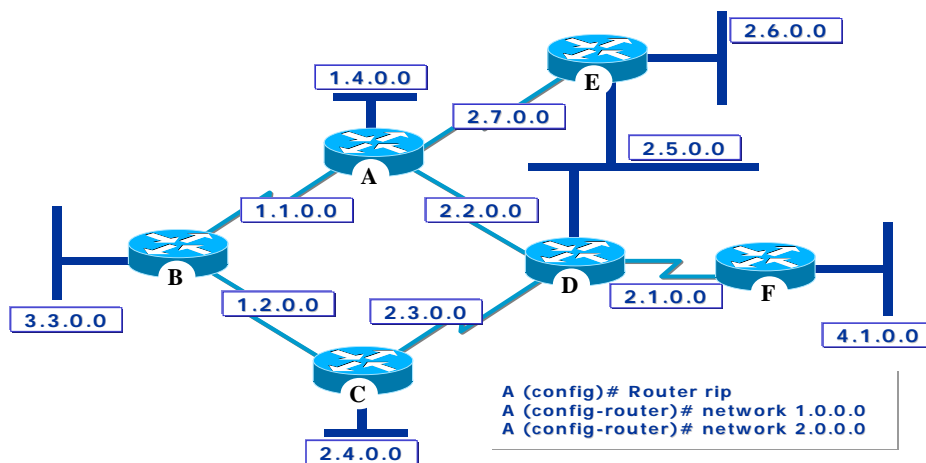
- 4.2 En el siguiente ejemplo:

- 4.2.1 **router rip**—Selecciona RIP como protocolo de enrutamiento

- 4.2.2 **network 1.0.0.0**—Especifica una red conectada directamente.

- 4.2.3 **network 2.0.0.0**—Especifica una red conectada directamente.

- 4.3 Las interfaces del router A de Cisco conectadas con las redes 1.0.0.0 y 2.0.0.0 enviarán y recibirán actualizaciones de RIP. Estas actualizaciones de enrutamiento permiten al router conocer la topología de la red.



MONITOREO RIP

- 4.4 El comando **show ip protocol** visualiza los valores de sincronizadores de enrutamiento e información de la red, asociados con todo el router. Es posible utilizar esta información para verificar la información de enrutamiento. Este router está enviando cada 30 segundos la información de la tabla de enrutamiento actualizada (este intervalo es configurable). La próxima actualización será enviada en 9 segundos. El router inyecta rutas para las redes mencionadas a continuación de la línea "enrutamiento para redes".

Tabla de enrutamiento IP

4.5 El comando **show ip route** visualiza el contenido de la tabla de enrutamiento IP. La tabla de enrutamiento contiene entradas para todas las redes y subredes conocidas, y contiene un código que indica cómo se adquirió esa información.

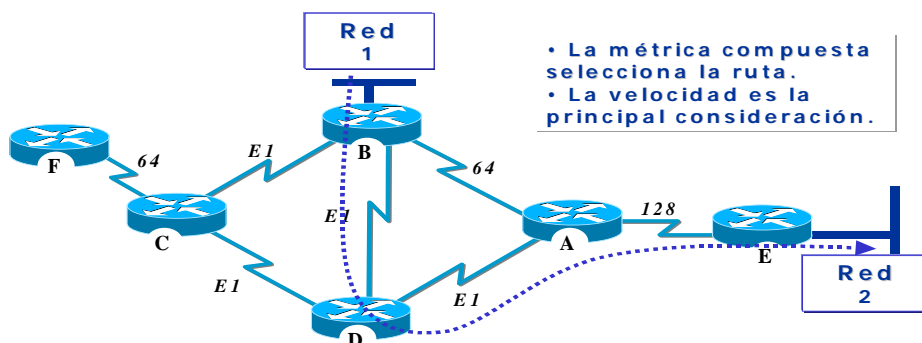
4.6 Todas las rutas hacia las redes que el router aprende le agrega la máscara correspondiente a la interface por la cual recibió la actualización (RIP versión 1).

DEBUG RIP

4.7 El comando **debug ip rip** muestra actualizaciones de enrutamiento RIP, mientras son enviadas y recibidas. En este ejemplo, la actualización es enviada y retransmitida por la interfaces seriales 0 y 2.

5. IGRP

5.1 IGRP es un protocolo de enrutamiento por vector de distancia desarrollado por Cisco. IGRP envía actualizaciones de enrutamiento (que no incluyen información de subredes) a intervalos de 90 segundos que publican redes para un sistema autónomo en particular. Corre directamente sobre IP (protocolo 88)



5.2 Las siguientes son algunas de las características claves de IGRP:

5.2.1 Versatilidad para manejar automáticamente topologías indefinidas y complejas.

5.2.2 Flexibilidad para los segmentos que tienen diferentes características de ancho de banda y retraso.

5.2.3 Escalabilidad para funcionar en redes muy grandes.

5.3 El protocolo de enrutamiento IGRP utiliza una combinación de variables para determinar una métrica compuesta. Las variables que utiliza IGRP incluyen:

5.3.1 Ancho de banda (B)

5.3.2 Retardo fijo entre nodos (D)

5.3.3 Carga por tráfico (L)

5.3.4 Fiabilidad ó tasa de error en el trayecto (R)

5.3.5 Unidad máxima de transmisión (MTU) ²¹

5.3.6 Cuenta de saltos hasta el destino (H)

METRICA IGRP

5.4 IGRP utiliza el conjunto de valores indicado para computar las rutas. Se aplica un algoritmo a dichos valores, ponderándolos mediante coeficientes K1, K2, K3, K4 y K5.²²

$$Métrica = (K1 * B) + \frac{K2 * B}{256 - L} + (K3 * D) * \frac{K5}{R + K4}$$

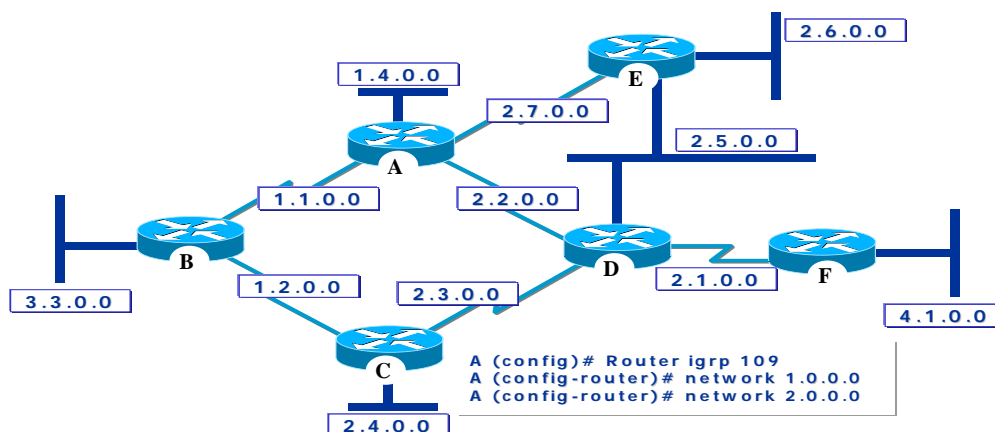
5.5 El B se halla dividiendo 10 millones por el menor de todos los anchos de banda [en Kbps] de las interfaces de salida (si el Bw=1,544 Mbps → 10000000/1544= 6476).

5.6 El D es la suma de todos los retardos de las interfaces de salida, dividido por 10 [decenas de microsegundos] (si los retardos son (20000 useg + 1000 useg)/10 = 2100)

5.7 La métrica sería entonces de 6476+2100= 8576. *El trayecto con la menor métrica es el mejor camino.*

Ejemplo de configuración de IGRP

5.8 En el siguiente ejemplo: se selecciona a IGRP como el protocolo de enrutamiento para el sistema autónomo 109. Todas las interfaces conectadas a las redes 1.0.0.0 y 2.0.0.0 utilizarán IGRP para reunir y distribuir información de enrutamiento.



5.8.1 router igrp 109—Selecciona a IGRP como el protocolo de enrutamiento para el sistema autónomo 109.

5.8.2 network 1.0.0.0—Especifica una red conectada directamente.

5.8.3 network 2.0.0.0—Especifica una red conectada directamente.

²¹ MTU - (*maximum transmission unit*) Unidad máxima de transmisión. Tamaño máximo de paquete, en bytes, que puede manejar una interface en particular.

²² Los defaults son K1 = K3 = 1, K2 = K4 = K5 = 0.

MONITOREO IGRP

5.9 El comando **show ip protocol** muestra el protocolo de enrutamiento IP, los temporizadores de enrutamiento y la información de la red asociada con todo el router.

5.10 El algoritmo utilizado para calcular la métrica de enrutamiento para IGRP también se muestra en esta pantalla. También incluye información acerca de las métricas de enrutamiento y filtros de enrutamiento.

Tabla de enrutamiento IP

5.11 El comando **show ip route** muestra los contenidos de una tabla de enrutamiento IP. La tabla contiene una lista de todas las redes y subredes conocidas y las métricas relacionadas con cada entrada.

DEBUG IGRP

5.12 El comando **debug ip igrp transactions** muestra actualizaciones de enrutamiento RIP, mientras son enviadas y recibidas.

```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on
RouterA#
00:21:06: IGRP: sending update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:21:06:      network 10.0.0.0, metric=88956
00:21:06:      network 192.168.1.0, metric=91056
00:21:07: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
00:21:07:      network 172.16.0.0, metric=1100
00:21:16: IGRP: received update from 10.1.1.2 on Serial2
00:21:16:      subnet 10.2.2.0, metric 90956 (neighbor 88956)
00:21:16:      network 192.168.1.0, metric 91056 (neighbor 89056)
```

CISCOWORKS SMNS

INTRODUCCIÓN

SERVIDOR CISCO WORKS

WHATS UP GOLD

RME

1. INTRODUCCIÓN

1.1 CiscoWorks Small Network Management Solution (CWSNMS) es una solución integral de administración de red para redes pequeñas a medianas con hasta 40 dispositivos Cisco. CWSNMS provee un conjunto poderoso de herramientas de configuración y monitoreo para administrar dispositivos Cisco.

Aplicaciones

1.2 CWSNMS incluye las siguientes aplicaciones:

1.2.1 CiscoWorks Server (In Common Services)

1.2.2 Resource Manager Essentials

1.2.3 CiscoView

1.2.4 WhatsUp Gold

CiscoWorks Server

1.3 CiscoWork Server es parte de CiscoWorks Common Services. Este servidor permite ejecutar tareas de administración de red comunes, tales como manejar cuentas de usuario, la base de datos, arrancar y detener los procesos del servidor CiscoWorks, etc.

1.4 También puede comprobarse la conectividad y accesibilidad de dispositivos y diagnosticar dispositivos con fallas.

Resource Manager Essencials

1.5 RME es un conjunto de aplicaciones basadas en web que ofrece soluciones para la administración de switches, servidores de acceso y routers Cisco. La interface browser de RME provee fácil acceso a la información crítica para mantener la operatividad de las redes, y simplifica la ejecución de tareas que, en modo manual, consumen mucho tiempo.

1.6 RME está basado en una arquitectura cliente/servidor que conecta múltiples clientes basados en web a un servidor en la red.

Cisco View

1.7 Básicamente, CV provee vistas gráficas de los paneles frontales y posteriores de los equipos. Las pantallas dinámicas y gráficos a color simplifican el monitoreo del estado de los dispositivos, componentes de diagnóstico específicos de los dispositivos, y su configuración.

1.8 CV puede lanzarse tanto desde el Device Center del escritorio de CWSMNS, o desde Whats Up Gold.

Whats Up Gold

1.9 Whats Up Gold (WUG) es un software de gestión de red de otro proveedor (Ipswitch Inc). WUG permite monitorear concurrentemente múltiples dispositivos sobre un mapa topológico (mientras que CV solamente tiene capacidad para monitorear un dispositivo por vez).

1.10 Por consiguiente, WUG permite el descubrimiento, mapeo, monitoreo y el rastreo de alarmas.

Desktop

1.11 El Desktop de CW es la interface hacia las aplicaciones de administración de red de CWSMNS. Es una interface gráfica de usuario (GUI) que corre sobre un web browser. El desktop ofrece las siguientes características:

1.11.1 Clientes Web

1.11.2 Invocación del Desktop

1.11.3 Logging In

1.11.4 Uso del Desktop

1.11.5 Ayuda en línea

1.12 Cada vez que la aplicación de administración de red sea invocada, CW verifica que el Plug-in Java requerido se encuentre instalado en el sistema cliente. Si así no estuviere, CW requerirá dicha instalación.

Clientes Web

1.13 El servidor puede ser accedido desde cualquier cliente que cumpla con los requerimientos del sistema apropiados. El único software cliente requerido es el web browser Microsoft Internet Explorer.

Uso del Desktop

1.14 El Desktop de CW es la interface de usuario primaria y el punto de partida para todas las tareas. Después de realizado el login, el desktop muestra las siguientes solapas:

1.14.1 WhatsUpGold

1.14.2 Essentials

1.14.3 Device Center

1.14.4 Admin

1.15 Cada una de las solapas de navegación contiene un grupo de enlaces, los cuales a su vez, contienen grupos de tareas asociadas o similares, herramientas, reportes y otras opciones.

Ayuda en línea

1.16 Cada aplicación de CW incluye ayuda en línea con información conceptual y de procedimiento, con el objetivo de facilitar la utilización. Además integra:

1.16.1 Un motor de búsqueda: Búsqueda de tópicos de ayuda por palabras clave.

1.16.2 Un índice: Presentación de tareas de red típicas.

1.16.3 Un glosario: Definición de términos de CW.

1.17 Si se encuentra seleccionada una opción en el árbol de navegación, aparece la ayuda para esa opción.

2. SERVIDOR CISCO WORKS

Conocimientos preliminares

2.1 CW es una familia de productos basados en los estándares de Internet para la administración de redes y dispositivos Cisco. Todos los productos CW utilizan y dependen del servidor CW. El servidor CW ejecuta un conjunto común de servicios de administración, los cuales son compartidos por múltiples aplicaciones de administración de red.

2.2 Adicionalmente, también provee a la administración de los roles y privilegios de los usuarios. Esto permite controlar el acceso a las aplicaciones y a funciones específicas dentro de las aplicaciones. El control de roles y privilegios, además de realizarse a través de servicios de autenticación y control incluidos en CW, también puede ejecutarse utilizando un servidor de autenticación externo.

Servidor y aplicaciones

2.3 Aún cuando muchas aplicaciones dependen del servidor CW, no todas utilizan los servicios con la misma extensión.

2.4 El servidor CW, básicamente provee dos tipos de servicios:

2.4.1 Runtime Services: Desktop, gestión de procesos, seguridad y el motor de ayuda en línea (se habilitan durante la instalación).

2.4.2 System Services: Motor y utilidades de base de datos, servicios de distribución de eventos y administración de tareas (jobs).

2.5 En tanto que los servicios Runtime están siempre habilitados por omisión, los servicios System son habilitados a partir de la instalación de algún software de aplicación que requiera dichos servicios. Finalmente, todas las aplicaciones son integradas por el Desktop.

Ejecución de tareas

2.6 La mayoría de las tareas, directamente requieren privilegios de nivel de administrador porque afectan la performance y el comportamiento del servidor CW. Solamente algunas tareas son accesibles a todos los usuarios.

Descripción
Verificación del estado del servidor
Configuración de la cuenta de usuario
Verificación del estado de procesos
Verificación del estado del archivo de log
Comprobación de conectividad (Nslookup)
Comprobación de conectividad (Traceroute)
Comprobación de conectividad (Ping)
Comprobación de conectividad (Estación-dispositivo)

Configuración del Servidor

2.7 El servidor CW incluye herramientas con el objeto de configurar el servidor apropiadamente para soportar otras aplicaciones Cisco.

2.7.1 Configuración de cuentas de usuario

2.7.2 Instalación del Plug-in Java

2.7.3 Restablecimiento de passwords

Configuración de cuentas de usuario

2.8 Varias operaciones de administración de redes y aplicaciones son potencialmente disruptivas para la red o las mismas aplicaciones y deben ser protegidas. Para prevenir que tales operaciones sean utilizadas accidental o maliciosamente, CW utiliza un sistema de seguridad multinivel que permite el acceso a ciertas funciones solamente a usuarios que puedan autenticarse con el nivel apropiado. CW provee dos IDs (identificaciones) de acceso predefinido, pero el administrador puede crear IDs adicionales:

2.8.1 Guest (se especifica una password durante la instalación, rol de usuario = Help Desk)

2.8.2 Admin (se especifica la password durante la instalación, rol de usuario = combinación de administrador del sistema, administrador de red, operador de red, aprobador y Help Desk). Equivalente al administrador de Windows para CW. Tiene acceso a todas las tareas de CW.

2.9 Los administradores del Sistema determinan los niveles de seguridad de los usuarios. Cuando se configura un usuario, también se le asigna uno o más roles.

2.10 El rol del usuario, o la combinación de roles, determinan cuales son las aplicaciones de CW que se presentan durante la navegación.

Nivel	Descripción
0	Mesa de ayuda [Help Desk]
1	Aprobador [Approver]
2	Operador de red [Network Operator]
4	Administrador de red [Network Administrator]
8	Administrador de Sistemas [System Administrator]
6	Exportación de datos [Export Data]
32	Desarrollador [Developer]

2.11 Los usuarios pueden realizar algunas tareas sobre sus propias cuentas, pero la mayoría de las tareas de seguridad requieren privilegios correspondientes al rol de administrador de sistemas.

2.12 Cuando se ejecuten tareas de seguridad, deben tenerse en cuenta las siguientes consideraciones:

2.12.1 RME no puede recuperar passwords olvidadas/perdidas. Se requiere un nivel de administrador de sistemas para cambiar la password, o borrarla, y luego volver a agregar el rol de usuario.

2.12.2 El usuario admin está reservado y no puede ser borrado.

2.12.3 Si se olvida la password de admin, debe acudir al utilitario indicado en “Restablecimiento de passwords”.

Tarea	Proposition	Nivel
Cambiar password	Modificar la contraseña de su propia cuenta.	Todos
Agregar usuario	Crear nueva cuenta y asignar nivel de acceso	Admin
Borrar usuario	Remover cuenta	Admin
Modificar usuario	Actualización de la información de usuario	Admin
Ver usuarios loggeados	Muestra información de usuarios activos y enviar mensajes	Admin

Restablecimiento de passwords

2.13 El utilitario de restablecimiento de passwords permite cambiar la password de un usuario local CW, desde la línea de comandos. Es indispensable poseer privilegios de administrador ó super usuario para ejecutar este utilitario.

Administración del Servidor

2.14 El servidor CW incluye herramientas administrativas para asegurar que el mismo se comporta adecuadamente. Entre ellas se encuentran:

- 2.14.1 Herramientas básicas
- 2.14.2 Mantenimiento de archivos de Log
- 2.14.3 Tareas de Administración de Datos
- 2.14.4 Gestión de Procesos de Back-end
- 2.14.5 Gestión de Trabajos y Recursos
- 2.14.6 Gestión de eventos de red

Herramientas básicas

2.15 Las herramientas administrativas básicas permiten realizar las siguientes tareas:

TAREA	PROPÓSITO
Visualizar paquetes de software instalados	Lista las aplicaciones instaladas
Visualizar el estado del archivo de log	Muestra el tamaño y la utilización del logfile

Mantenimiento de archivos de log

2.16 Los archivos de registro de actividades (log files) pueden crecer y agotar el espacio en disco. CW incluye un script que permite controlar este crecimiento.

2.17 El script está escrito para mantener los siguientes archivos:

2.17.1 Daemon manager

2.17.2 JRUN

2.17.3 Web server log files

Tareas de administración de datos

2.18 Regularmente deben ejecutarse tareas de administración del almacenamiento para asegurarse de que existan backups de la base de datos en caso de que la misma se torne inutilizable o corrompida.

2.19 Al configurar la estrategia de backup de la base de datos, deben considerarse los siguientes lineamientos:

2.19.1 Las tareas de resguardo y restauración de los datos solamente están soportadas dentro de una misma versión (no puede recuperarse una base resguardada con otra versión).

2.19.2 Chequear el tamaño de los archivos almacenados en el directorio de backup. Algunos de ellos podrían requerir mayor espacio en disco.

2.19.3 Los archivos de la base de datos se almacenan utilizando la siguiente estructura de directorios de backup:

2.20 El nombre de suite utilizada por los archivos de base de datos del servidor CW es cmf. La base de datos .cmf incluye el backup de datos de las aplicaciones del servidor CW.

TAREA	PROPÓSITO
Backup de la base de datos	Ejecutar una tarea de backup en este momento.
Programación de backups regulares	Ejecutar tareas de backups en forma programada
Restore de una base de datos	Reemplazar la base de datos actual con otra copia
Cambio de password de la base de datos	Cambiar la password de la base de datos por seguridad

Backup de datos

2.21 Es posible realizar el backup de los datos a la demanda, en lugar de aguardar el próximo backup programado, con la opción “Back up Data Now”.

Gestión de procesos de back-end

2.22 Las aplicaciones CW utilizan procesos de back-end para administrar actividades o trabajos específicos de las aplicaciones. Las herramientas de administración de procesos posibilitan el control de estos procesos para optimizar ó diagnosticar el servidor CW.

TAREA	PROPÓSITO
Arrancar proceso	Reiniciar procesos específicos
Detener proceso	Detiene procesos específicos
Ver procesos	Mostrar información de procesos incluyendo estado, ID y otros datos.

TAREA	PROPÓSITO
Ver fallas de procesos	Muestra los procesos con fallas, información de fallas, y hora de ocurrencia de la falla.

Gestión de Trabajos y Recursos

2.23 La gestión de trabajos (Job Management) provee servicios de notificación de trabajos, recursos y eventos a CW. Se utiliza el Job Management para mostrar trabajos, liberar recursos y detener y/o remover trabajos.

TAREA	PROPÓSITO
Cancelar un trabajo programado	Detiene la ejecución de un trabajo, pero lo mantiene en el Job Management
Remover un trabajo	Remueve un trabajo del Job Management
Destruir un recurso huérfano	Libera recursos trabados por fallas en el sistema. Sólo debe utilizarse si no existen otras opciones.

Gestión de eventos de red

2.24 Existen dos servicios de CW que permiten la administración de eventos. Las aplicaciones utilizan uno u otro.

2.24.1 Event Distribution Service (EDS)

2.24.2 Event Services Software (ESS)

Event Distribution Service (EDS)

2.25 EDS permite administrar las fuentes y los destinatarios de los eventos. Las fuentes de eventos crean los eventos de red, mientras que los destinatarios son los consumidores de estos eventos

Fuente = originador = creador

Destino = consumidor

TAREA	PROPÓSITO
Habilitar o deshabilitar el debugging o la generación de mensajes de trace	Diagnosticar problemas
Configurar servicios individuales	Habilita el setup y la configuración de fuentes de eventos, o servicios destino de eventos, tales como parámetros de colas.
Asociar filtros de eventos a un consumidor genérico.	Permite utilizar un filtro para especificar qué eventos deben pasarse a cada consumidor genérico.
Ver estadísticas de performance de todas las colas de datos internas de las fuentes y consumidores de eventos.	Muestra el trabajo que está realizando EDS. A partir de estas estadísticas puede determinarse si se están perdiendo eventos y la marca máxima para fijar la capacidad de la cola.
Ver eventos recibidos por EDS y el logger de eventos.	Monitorea o diagnostica la red.

Event Services Software (ESS)

2.26 ESS provee los medios para que varios procesos de CW puedan enviar mensajes broadcast a otros procesos en un ambiente de red distribuido. ESS utiliza un modelo de publicación y suscripción, donde existen procesos que realizan broadcast de mensajes, mientras que otros, seleccionadamente, se suscriben a los mensajes. En este modelo, cada proceso se suscribe a un host de tópicos, y otros procesos, cuando necesitan que algún proceso reciba el mensaje, publican sus mensajes a alguno de estos tópicos. Por ejemplo, si el proceso 1 está suscrito a los tópicos a, b y c, otros procesos publicarán mensajes destinados al proceso 1 sobre los tópicos a, b ó c.

3. WHATS UP GOLD

3.1 Whats Up Gold (WUG) es un software de gestión de red de otro proveedor (Ipswitch Inc). WUG permite monitorear concurrentemente múltiples dispositivos sobre un mapa topológico (mientras que CV solamente tiene capacidad para monitorear un dispositivo por vez).

3.2 Por consiguiente, WUG permite el descubrimiento, mapeo, monitoreo y el rastreo de alarmas.

Roles de usuario

3.3 CWSNMS crea dos usuarios privilegiados en WUG: admin y guest. Estos privilegios permiten utilizar un único login para las dos aplicaciones.

3.4 El usuario admin de WUG es mapeado con los roles del Administrador de Red y del Administrador de Sistemas del servidor CW.

3.5 El usuario guest de WUG es mapeado con los otros roles de CW, tales como Help Desk, Operador de red, etc.

Mapeos

3.6 El mapeo EssentialsmanagedDevices contiene los dispositivos gestionados por la base de datos de RME. No puede importarse este mapeo a RME, sino que es creado automáticamente la primera vez, ya sea que:

3.6.1 Se agreguen o importen dispositivos

3.6.2 Se descubran dispositivos utilizando la consola de WUG y luego se utilice la opción “Export to Essentials”.

3.7 Subsecuentemente, cada vez que se agreguen dispositivos a RME utilizando la opción “Recreate Map”, deberá actualizarse manualmente el mapeo. Pueden ejecutarse las siguientes tareas con SNMS WUG en el Desktop de CW:

3.7.1 Recreate Map

3.7.2 Export to Essentials

3.7.3 Lanzar las aplicaciones Device Center y CiscoView

3.7.4 Cambiar las passwords de los usuarios *admin* y *guest*.

Passwords

- 3.8 CW SMNS crea dos cuentas de usuarios privilegiados en WUG: *admin* y *guest*.
- 3.8.1 El usuario *admin* de WUG es mapeado con los roles del Administrador de Red y del Administrador de Sistemas del servidor CW.
- 3.8.2 El usuario *guest* de WUG es mapeado con los otros roles de CW, tales como Help Desk, Operador de red, etc.
- 3.9 Es posible utilizar estos dos IDs de usuario para acceder al servidor de web:
- 3.9.1 ID de usuario *admin*: Posee acceso completo a todas las funciones y vistas de WUG. La password de *admin* se genera durante la instalación del producto.
- 3.9.2 ID de usuario *guest*: Posee acceso a todas las vistas de WUG pero no puede cambiar ninguna configuración. La password de *guest* se genera durante la instalación del producto.

Generación de mapas

- 3.10 Dentro de las tareas de administración figura el descubrimiento de dispositivos en la red y la creación del mapa EssentialsManagedDevices, utilizando la aplicación WUG (se utiliza la consola WUG y el enlace WUG en el Desktop de CWSNMS).

4. RME

Introducción

- 4.1 RME es un conjunto de aplicaciones basadas en web que ofrece soluciones para la administración de switches, servidores de acceso y routers Cisco. La interface browser de RME provee fácil acceso a la información crítica para mantener la operatividad de las redes, y simplifica la ejecución de tareas que, en modo manual, consumen mucho tiempo.
- 4.2 RME está basado en una arquitectura cliente/servidor que conecta múltiples clientes basados en web a un servidor en la red. A medida que el número de dispositivos de red aumenta, pueden agregarse servidores adicionales o puntos de colección de datos para manejar el crecimiento de la red con el mínimo impacto sobre la aplicación browser del cliente.
- 4.3 Aprovechando la inherente escalabilidad de la arquitectura intranet, RME soporta múltiples usuarios conectados desde cualquier parte de la red. La infraestructura basada en web permite el acceso concurrente a las herramientas de gestión de red, aplicaciones y servicios, de operadores, administradores, técnicos, personal de Help Desk, administradores IS, y usuarios finales.
- 4.4 RME permite que los administradores de la red puedan visualizar y actualizar el estado y la configuración de todos los dispositivos Cisco desde cualquier punto de la red, mediante un browser estándar que actúa como cliente de RME. RME mantiene una base de datos con la información de red actualizada. Puede generar una gran variedad de reportes utilizables para el diagnóstico y la planificación de la capacidad.
- 4.5 Aún cuando los dispositivos son agregados al inventario de RME al iniciarse la aplicación, el administrador puede programar la exploración y actualización periódica de la información de los dispositivos para asegurarse de que la información almacenada es la más reciente. Adicionalmente, RME registra automáticamente cualquier cambio realizado sobre los dispositivos de la red, facilitando la tarea de identificar los cambios y el responsable de los mismos.

4.6 Las aplicaciones RME proveen al monitoreo y control de fallas de la red, así como herramientas prácticas para administrar imágenes de software y configuraciones en routers y switches. Las aplicaciones RME, juntamente con los enlaces a los servicios y el soporte de Cisco.com, automatizan el mantenimiento del software para facilitar el control y el soporte de la red.

Características

4.7 RME trabaja en conjunción con el servidor CW, el cual contiene un conjunto de servicios de administración compartidos por múltiples aplicaciones de gestión. Estos servicios de gestión son habilitados cuando se instala una suite y se abre alguna aplicación que depende de alguno de estos servicios.

4.8 Si alguna suite particular de aplicaciones no utiliza un servicio o no lo utiliza en toda su extensión disponible, ese servicio podría no aparecer en el Desktop de CW.

4.9 RME utiliza los siguientes servicios de CW:

4.9.1 Motor y utilidades de base de datos

4.9.2 Desktop para login y lanzamiento de aplicaciones

4.9.3 Gestión de eventos

4.9.4 Sistema de ayuda en línea

4.9.5 Gestión de trabajos (Jobs)

4.9.6 Gestión de Procesos

4.9.7 Seguridad

4.9.8 Servidor de web

Componentes de RME

4.10 La infraestructura basada en web de RME esta integrada por los siguientes componentes:

4.10.1 *CiscoWorks Server*: RME depende de CW para las funciones comunes, tales como el motor de base de datos, ayuda en línea, seguridad, login, lanzamiento de aplicaciones, gestión de trabajos y procesos, y el servidor de web. Provee un marco de trabajo común e interface para todos los productos CiscoWorks. El servidor CW debe permanecer en línea constantemente para sondear los dispositivos, monitorear eventos, y realizar la recolección programada de datos. Si el servidor se cae, se producirá una interrupción en el flujo de información recibido y almacenado por RME.

4.10.2 *Base de datos y funciones de RME*: RME almacena toda la información crítica de gestión de red en una base de datos central, incluyendo el inventario de dispositivos, imágenes de software, archivos de configuración, mensajes de syslog, y registro de cambios. Las funciones de RME interactúan con la base de datos y con los dispositivos de red para recoger la información, mostrar reportes, y automatizar muchas tareas repetitivas. Muchas funciones de RME pueden configurarse para sondear periódicamente los dispositivos y actualizar la base de datos automáticamente. RME utiliza protocolos comunes como SNMP, Telnet, TFTP y RCP para acceder a los dispositivos y recuperar archivos de configuración e imágenes.

4.10.3 *Cisco.com*: RME también se conecta al sistema Cisco.com para obtener actualizaciones de producto e información de asistencia técnica. El acceso a Cisco.com no es mandatorio para RME, pero aumenta sus capacidades. Las funciones de Software Management requieren acceso a Cisco.com.

Aplicaciones y tareas

4.11 Es posible ejecutar una extensa variedad de tareas con las siguientes aplicaciones suministradas por RME:

- 4.11.1 Vistas: [Device Views]
- 4.11.2 Auditoría de cambios: [Change Audit]
- 4.11.3 Gestión de configuraciones: [Configuration Management]
- 4.11.4 Inventario: [Inventory]
- 4.11.4 Aprobación de trabajos: [Job Approval]
- 4.11.5 Gestión de software: [Software Management]
- 4.11.6 Análisis del Syslog: [Syslog Analysis]

Vistas

4.12 RME provee vistas de dispositivos –agrupamientos lógicos utilizados para especificar un dispositivo o grupo de dispositivos. Pueden definirse vistas para agrupar dispositivos seleccionados en un grupo lógico.

4.13 Por ejemplo una vista de dispositivos permite ver, rápidamente, reportes relacionados con los dispositivos de un cierto tipo, o con características específicas, tales como switches Catalyst, o los dispositivos por los que un operador tiene responsabilidad.

4.14 Dado que casi todas las tareas de RME requieren se defina el conjunto de dispositivos sobre los cuales deben ejecutarse, las vistas proveen una forma conveniente de crear grupos de dispositivos. Por ejemplo, antes de desplegar un reporte de inventario, deben seleccionarse los dispositivos a incluir en el reporte. Las vistas pueden acelerar la selección (en lugar de ejecutar el reporte por cada dispositivo). La performance de la interface gráfica (GUI) de RME puede verse afectada si el número de dispositivos seleccionados en la vista es demasiado grande. Debe evitarse incluir en la vista a “todos los dispositivos” cuando el número de dispositivos del inventario es muy grande. Lo más práctico es utilizar vistas de sistema, o crear vistas personalizadas para mantener las vistas con un número de dispositivos manejable.

Tipos de Vistas

4.15 Existen tres categorías de vistas de dispositivos:

4.15.1 *System Views*: Están predefinidas y disponibles inmediatamente después de la instalación de RME. Incluyen la mayoría de las familias de dispositivos Cisco.

4.15.2 *Custom Views*: Definidas por los usuarios, y pueden ser utilizadas por todos los demás usuarios con acceso al servidor.

4.15.3 *PrivateViews*: Definidas por los usuarios, pero solamente pueden ser utilizadas por el usuario que las creó.

4.16 Además, pueden crearse dos tipos diferentes de vistas dentro de la categoría de vistas custom o privadas:

4.16.1 *Dynamic Views*: Son agrupamientos lógicos basados en los atributos de los dispositivos, tales como la clase de dispositivo o la versión de software. Los dispositivos en una vista dinámica pueden cambiar en base al valor de los atributos en el inventario. Por ejemplo, una vista dinámica puede ser la de todos los dispositivos con la versión IOS 12.0. Todas las vistas de sistema ó System Views son dinámicas.

4.16.2 *Static Views*: Son agrupamientos lógicos basados en características definidas por los usuarios. Incluyen a cualquier dispositivo que desee agregarse a la vista. Los miembros del grupo no cambian, a menos que se agreguen o remuevan dispositivos. Debe utilizarse vistas estáticas cuando no se desea que la membresía cambie automáticamente.

Auditoría de cambios

4.17 Las aplicaciones de auditoría de cambios permite rastrear y reportar los cambios en la red. Provee capacidades para que otras aplicaciones puedan loggear información de cambios a un repositorio central.

4.18 Los cambios de Inventario incluyen cualquier modificación realizada sobre la información de los dispositivos almacenada en la base de datos de Inventario, tales como chasis, interfaces e información del sistema.

4.19 Los cambios de Software incluyen actualizaciones a nuevas imágenes de software.

4.20 Los cambios de Configuración incluyen todas las modificaciones realizadas en los archivos de configuración de los dispositivos, tanto si fueron realizado utilizando la funcionalidad de RME, o aún cuando se realizaren externamente a estas funciones.

4.21 Los cambios enviados por los administradores de configuración y de software no pueden ser filtrados. Es posible visualizar los registros de cambios, o realizar búsquedas específicas por tipo, características o tiempo. Puede programarse la eliminación de registros de cambios antiguos.

4.22 Y también puede configurarse para enviar los registros de cambios, bajo la forma de traps SNMP a servers remotos, para monitorear y visualizar cambios desde estaciones de gestión de red remotas con capacidades de recolección de eventos.

4.23 Los registros son almacenados en la base de datos de RME hasta que son borrados, y se requiere un mantenimiento continuo para eliminar los registros antiguos de la base de datos. Gestión de configuraciones

4.24 La aplicación de gestión de configuraciones [Configuration Management] almacena los archivos de configuración (la actual y el número de versiones previas especificadas) de todos los dispositivos Cisco existentes en el Inventario.

4.25 Además, rastrea los cambios y actualiza automáticamente la base de datos. A veces, cambios en la configuración de un dispositivo puede conducir a fallas o problemas de performance en la red. Configuration Management es de gran ayuda para simplificar y automatizar tareas repetitivas de alto consumo de tiempo.

4.26 Cuando se realiza un cambio en la configuración de un dispositivo, se genera un evento automático al fichero que recolecta el último archivo de configuración.

4.27 Por ejemplo, para mejorar la performance de NetConfig, podría utilizarse Telnet para descargar configuraciones al dispositivo y TFTP para explorar las configuraciones.

4.28 Para descargas de configuraciones, los protocolos utilizados son Telnet y SSH (con ese orden, aunque puede cambiarse).

4.29 Para la exploración de configuraciones, los protocolos utilizados son: TFTP, Telnet, RCP y SSH (con ese orden, aunque puede cambiarse).

4.29.1 Verificar los requerimientos de los dispositivos para asegurarse de que RME puede comunicarse con los dispositivos.

4.29.2 Crear listas de aprobadores (si se requieren instancias de aprobación previa de los cambios de configuración) y establecer las preferencias del Fichero de Configuración (programación de actualizaciones, número de copias a mantener, etc.).

4.29.3 Utilizar el Fichero de Configuración (Configuration Archive) para visualizar las configuraciones de los dispositivos e identificar/planificar los cambios necesarios. Luego, pueden utilizarse las aplicaciones NetConfig y Config Editor para ejecutar y confirmar los cambios.

4.29.4 Realizar, como mantenimiento continuo, el chequeo del reporte Configuration Sync para asegurar que todas las configuraciones running y startup son iguales para cada uno de los dispositivos.

4.30 El Administrador de la red puede utilizar los comandos Network Show y reportes customizados para diagnosticar problemas y recoger información.

Inventario

4.31 Las redes son una combinación de sistemas heterogéneos, geográficamente dispersos. Mantener el control de inventario de los activos de hardware y software es una tarea crítica. Además, la mayoría de las tareas de RME se ejecutan sobre conjuntos de dispositivos, por lo tanto la información precisa de los dispositivos debe residir en la base de datos de RME.

4.32 El Inventory Manager tiene la responsabilidad de mantener el inventario. Como RME utiliza diferentes servicios de gestión para recolectar la información de los dispositivos (SNMP, TFTP, Telnet, RCP), cada dispositivo existente en la base de datos (Inventario) debe incluir los parámetros (atributos) de los servicios de gestión (cadena de comunidad, passwords). Cuando esta información existe en el Inventario, se considera que el dispositivo constituye un objeto gestionado por RME.

4.33 Es decir que mientras RME no disponga de la información de los atributos, ese dispositivo no estará bajo el control de RME. RME no realiza el auto-descubrimiento de dispositivos en la red, sino que deben ser agregados manualmente o importados en la base de datos de Inventario.

4.34 Para simplificar el proceso de población de la base de datos de Inventario, la información de los dispositivos puede importarse desde un archivo con formato de texto.

Gestión de Software

4.35 La aplicación de Software Management automatiza los pasos asociados con la planificación, programación y descarga de imágenes de software, y el monitoreo de la red.

4.36 Provee herramientas para almacenar copias de backup de todas las imágenes que corren en los dispositivos de la red. Además puede almacenar copias adicionales que se desee mantener, y planificar y ejecutar upgrades a varios dispositivos concurrentemente.

4.37 La aplicación puede analizar dispositivos e imágenes de software para determinar la compatibilidad y realizar recomendaciones antes del upgrade. Los reportes de Software Management permiten controlar todos los upgrades de versiones de la red.

4.38 Las imágenes deben importarse a RME para ser mantenidas en la Software Image Library. Inicialmente, las imágenes pueden ser importadas desde los mismos dispositivos de la red (o de otra fuente) para crear una copia de backup base de todos los dispositivos.

4.39 Además, después de la importación, puede configurarse a Software Management para que sondee periódicamente los dispositivos de la red para producir reportes ante la existencia de imágenes corriendo en la red que no se hallan almacenadas en la base de datos de RME.

Análisis del Syslog

4.40 La aplicación Syslog Analysis permite registrar eventos en forma centralizada y controlar los mensajes de error del sistema de los dispositivos Cisco. Los mensajes de error son utilizados para analizar la performance de los dispositivos y de la red.

4.41 Pueden almacenarse, como máximo, 1 millón de mensajes y hasta 14 días.

4.42 Es posible realizar el backup de los mensajes purgados en una ubicación especificada (formato CSV). Está permitido seleccionar el tamaño del archivo de backup, y una dirección de e-mail para recibir un aviso si el tamaño del backup excede el indicado.

4.43 Los mensajes recibidos por el servidor RME son periódicamente leídos (cada 30 segundos) por el proceso de análisis [Syslog Analyzer], donde se aplican filtros definidos por el usuario y el resultado se almacena en la base de datos de mensajes de Syslog de RME, y quedan disponibles para obtener reportes e iniciar scripts definidos por el usuario.